Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce

TESIS

Para optar el Título Profesional de Ingeniera en Telecomunicaciones

AUTOR

Jeniffer Reyna QUISPE CCUNO

ASESOR

Daniel DÍAZ ATAUCURI

Lima, Perú

2019

Referencia bibliográfica

Quispe, J. (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce*. Tesis para optar el título profesional de Ingeniera en Telecomunicaciones. Escuela Profesional de Ingeniería de Telecomunicaciones, Facultad de Ingeniería Electrónica y Eléctrica, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

Código Orcid del autor (dato opcional):

0000-0001-9844-1725

Código Orcid del asesor o asesores (dato obligatorio):

0000-0001-5747-2795

DNI del autor:

07139361

Grupo de Investigación:

Aplicaciones de las Tecnologias de Información y Comunicaciones

Institución que financia parcial o totalmente la investigación:

Vicerrectorado de Investigación y Posgrado

Ubicación geográfica donde se desarrolló la investigación. Debe incluir localidades y coordenadas geográficas.

Distrito, Ciudad: Surquillo, Lima

Latitud, Longitud: -12.11029, -77.010246

Año o rango de años que la investigación abarcó:

1 año

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA

ACTA DE SUSTENTACIÓN N° 005-VDAC-UMRAGT-FIEE/2019

TESIS N° 005-FIEE/2019 PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE TELECOMUNICACIONES

Los suscritos Miembros de Jurado, nombrados por la Dirección de la Escuela Profesional de Ingeniería de Telecomunicaciones de acuerdo a la Resolución Rectoral N° 03823-R-17, reunidos en la fecha bajo la Presidencia del Mg. Jesús Otto Villanueva Napuri e integrado por los Ingenieros: Ing. Esequiel Zavala Huavel, Mg. Wilbert Chávez Irazábal y el Ing. Daniel Díaz Ataucuri (Miembro - Asesor)

Después de escuchar la Sustentación de Tesis de la Bachiller **QUISPE CCUNO, Jeniffer Reyna (12190253),** para optar el Título Profesional de Ingeniera de Telecomunicaciones por la modalidad de Titulación Ordinaria, quien expuso su **TESIS: "IMPLEMENTACIÓN DE UN PROTOTIPO DE MONITOREO DE DISPOSITIVOS DE COMUNICACIÓN Y USUARIOS FINALES UTILIZANDO EL PROTOCOLO SNMP BASADA EN SOFTWARE LIBRE PARA UNA EMPRESA E-COMMERCE".**

Se acordó....aprobar.....por....unanimidad.....

Con la Nota de.....Dieciocho (18).....( )

Ciudad Universitaria, 25 de setiembre de 2019

Mg. Jesús Otto Villanueva Napuri
Presidente de Jurado

Ing. Esequiel Zavala Huavel
Miembro de Jurado

Mg. Wilbert Chávez Irazábal
Miembro de Jurado

Ing. Daniel Díaz Ataucuri
Miembro de Jurado-Asesor

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
DIRECCIÓN DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES

Mg. Jesús Otto Villanueva Napuri
Director de la EPIT

Dr. Víctor Manuel Cruz Ornetta
Decano FIEE – UNMSM

No basta saber, sino también aplicar el saber; no basta querer, es preciso obrar.

Johann Wolfgang von Goethe

DEDICATORIA

El presente proyecto de tesis está dedicado a Dios por todas las bendiciones recibidas; a mis padres, hermano, tío por brindarme todo su apoyo, comprensión, entusiasmo y a mi asesor de tesis, Mg. Daniel Díaz Ataucuri quien me brindó constantemente su apoyo disponiendo de su valioso tiempo y dirección sabia durante el proceso y desarrollo de la investigación para la presente tesis.

AGRADECIMIENTOS

Agradezco al Vicerrectorado de Investigación y Posgrado (VRIP) por la oportunidad que me brindaron al formar parte del programa de Promoción de Tesis Pre Grado, apoyo que propició y promovió el desarrollo de la investigación para la presente tesis.

Agradecer además al Instituto de Investigación de la FIEE, al brindarme las facilidades necesarias en diversas actividades académicas.

Agradecimiento especial a mi asesor de tesis, Mg. Daniel Díaz Ataucuri quien gracias a su guía, orientación, motivación, consejos y trabajo en conjunto ha sido posible el desarrollo y presentación de la presente tesis.

Finalmente agradezco a mi familia, seres humanos de gran valor e importancia en mi vida, quienes estuvieron a mi lado todo el tiempo, brindándome su apoyo incondicional en todas y cada una de las actividades realizadas para alcanzar este objetivo trascendental en mi vida académica y profesional.

RESUMEN

El propósito del trabajo de investigación es desarrollar e implementar un prototipo que permita monitorear en tiempo real los dispositivos de comunicación (router, switches, acces point) y los usuarios finales (laptop, computadoras personales, impresoras, fotocopiadoras) utilizando el protocolo Simple Network Management Protocol-SNMP y software libre para una empresa dedicada a la compra, venta y distribución de productos y servicios a través de Internet (e-commerce), con el fin de mejorar su productividad.

El prototipo propuesto permite que el especialista en el área de Redes y Comunicaciones (Seguridad Perimetral) tenga el control a través de las alertas y reporte de eventos de los diferentes equipos de comunicación cuando presente fallas o alguna anomalía en el funcionamiento normal de dichos dispositivos. Para realizar este control, el prototipo supervisa toda la actividad de la red de la empresa a través de un sondeo para conocer periódicamente el estado de los nodos de la red, haciendo uso del protocolo ICMP (protocolo de mensajes de control de internet) y los servicios en esos nodos, ya sea mediante sondeos específicos del protocolo SNMP que realizan una prueba para observar si el recurso responde correctamente o una conexión simple de puerto TCP/IP al puerto correspondiente. Los diferentes eventos presentados en la topología de red serán presentados a través de un reporte gráfico donde indica la disponibilidad de los equipos, con ello se tomará las decisiones inmediatas para la continuidad del negocio. La solución propuesta ha sido implementada bajo GNU/LINUX lo cual brinda facilidades en cuanto a costo de proyecto, aprendizaje de un nuevo sistema operativo, personalización del monitoreo para finalmente obtener los resultados esperados con el objetivo de mejorar el rendimiento de la empresa. La contribución importante de esta tesis es su aplicación en resolver la necesidad de monitorear la red de comunicación de una empresa dedicada a la distribución de productos y servicios a través de Internet.

Palabras claves: Prototipo, SNMP, Software Libre, Empresa, e-Commerce, GNU/LINUX.

SUMMARY

The purpose of the research work is to develop and implement a prototype that allows monitoring in real time the communication devices (router, access point, switches) and end users (laptop, personal computers, printers, photocopiers) using the Simple Network protocol Management Protocol-SNMP and free software for a company dedicated to the purchase, sale and distribution of products and services through the Internet (e-commerce), in order to improve their productivity.

The proposed prototype allows the specialist in the area of Networks and Communications (Perimeter Security) to have control through the alerts and report of events of the different communication equipment when there are faults or some anomaly in the normal operation of said devices. To carry out this control, the prototype monitors all the activity of the company's network through a survey to periodically know the status of the nodes of the network, making use of the Internet control message protocol (ICMP) and the services in those nodes, either through specific SNMP protocol polls that perform a test to see if the resource responds correctly or a simple TCP / IP port connection to the corresponding port. The different events presented in the network topology will be presented through a graphic report indicating the availability of the equipment, with this the immediate decisions will be taken for business continuity. The proposed solution has been implemented under GNU / LINUX which provides facilities in terms of project cost, learning a new operating system, customization of the monitoring to finally obtain the expected results in order to improve the performance of the company. The important contribution of this thesis is its application in solving the need to monitor the communication network of a company dedicated to the distribution of products and services through the Internet.

Keywords: Prototype, SNMP, Free Software, Company, e-Commerce, GNU / LINUX.

ÍNDICE

ÍNDICE DE FIGURAS

Capítulo II. MARCO TEÓRICO

Capítulo III. PROPUESTA DE LA TESIS

Capítulo IV. RESULTADOS

ÍNDICE DE TABLAS

Capítulo III.

ABREVIACIONES

AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
ASN	Abstract Syntax Notation
BER	Basic Encoding Rules
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DVR	Digital Video Recorder
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTP	File Transfer Protocol
GPL	General Public License
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
IP	Internet Protocol
IPSEC	Internet Protocol security
ISP	Internet Service Provider
JDBC	Java Database Connectivity
JMX	Java Management eXtensions
JSON	JavaScript Object Notation
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MIB	Management Information Base

MPLS	Multiprotocol Label Switching
NMM	Network Management Model
NMS	Network Management Systems
NRPE	Nagios Remote Plugin Executor
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
QoS	Quality of Service
RDP	Remote Desktop Protocol
RFC	Request For Comments
SA	Security Association
SDN	Software Defined Networking
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SYSLOG	System Logging
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WMI	Windows Management Instrumentation
XML	eXtensible Markup Language
XMP	Extensible Metadata Platform

CAPITULO I

OBJETIVOS DE LA TESIS

1.1 INTRODUCCION

Las redes de telecomunicaciones locales permiten que cualquier tipo de información útil relacionado al estado de la red, traducido en datos, pueda aportar de manera eficiente en el análisis del comportamiento de los diferentes dispositivos de comunicación y equipos finales que conforman una red de datos, en beneficio y satisfacción de los clientes al permitir la continuidad de los servicios que hacen uso. Por lo tanto, surge la necesidad que estas empresas cuenten con sistemas de monitoreo de la red en tiempo real, para conocer el estado de los diferentes dispositivos que constituye dicha red: los routers, switches, access point, los enlaces o nodos e incluso saber si un determinado usuario está o no activo.

El propósito de esta tesis es diseñar e implementar un prototipo de monitoreo de red usando software libre para mejorar el control de los dispositivos de comunicación que alberga la empresa para los diferentes servicios que ofrece. Esta herramienta permite que el especialista en el área de Redes y Comunicaciones (Seguridad Perimetral) tenga el control, a través de las alertas y reportes de eventos, de los diferentes equipos de comunicación cuando presente fallas o alguna anomalía en el funcionamiento normal de dichos dispositivos. El prototipo de monitoreo de red supervisa los servicios mediante sondeos específicos del protocolo SNMP en la que realiza una prueba para diagnosticar si el recurso responde correctamente o si existe una conexión de puerto TCP/IP.

1.2 JUSTIFICACION DE LA INVESTIGACION

Toda empresa que tenga información en tiempo real de los clientes conectados y del estado de los dispositivos que conforman su red hará posible una mejor toma de decisión.

Un corte del servicio de telecomunicaciones que no se detecta en el momento preciso, ocasionará inevitablemente pérdidas económicas.

El crecimiento de una empresa e-commerce, con la expansión de sus servicios, requiere un sistema de monitoreo y emisión de reportes con las notificaciones de eventos (network and outages) de una manera flexible, personalizable y de bajo costo.

Los centros de comunicaciones cumplen un rol importante dentro de la infraestructura de la empresa pues concentran los recursos tecnológicos necesarios para el procesamiento de datos, brindando garantías de disponibilidad, confidencialidad e integridad de la información, siendo crítica la necesidad del correcto monitoreo y control de sus componentes.

La presente tesis tiene como objetivo analizar, diseñar e implementar un prototipo de un sistema de monitoreo para una red de datos de una empresa e-commerce, de costo mínimo y flexible, utilizando el protocolo SNMP estandarizada por la IETF (Internet Engineering Task Force). Los beneficios tangibles que se obtendrán de esta investigación son:

- ✓ Ofrecer una alternativa de software de código abierto a un software licenciado.
- ✓ Correcto control de alertas y manejo de notificaciones de manera personalizada.
- ✓ Brindar notificaciones personalizadas de eventos de hardware y software.

Los agentes o actores que apreciarán directamente el impacto de la solución propuesta son:

- El administrador de red, encargado del control preventivo y correctivo.
- Los usuarios administrativos y el personal de la empresa.
- Los clientes quienes ponen a prueba el desempeño de los servicios ofrecidos.

En el caso de una empresa que realiza una migración de ISP (proveedor de servicios de internet) que no cuenta más con las herramientas de monitoreo

brindados por el ISP que deja, necesita un sistema de alerta de los diferentes eventos que se presentan dentro de su infraestructura.

La idea de implementar un prototipo de un sistema de monitoreo de la red basado en software libre nace precisamente de la necesidad de contar con una herramienta que no pertenezca al ISP (proveedor de la empresa) y que permita además brindar resultados imparciales a través de las notificaciones de los eventos. El presente prototipo de sistema de monitoreo, luego de una exhaustiva revisión y análisis profundo, puede ser implementado en producción, tras haber sido sometido a pruebas de calidad del servicio, en cualquier empresa.

1.3 ESTADO DEL ARTE

Según J. Zhang [1], 2017, "Los sistemas de monitoreo de red en tiempo real son muy importantes porque garantizan la seguridad y mantienen la estabilidad de la red. El protocolo ampliamente utilizado es el *Simple Network Management Protocol*-SNMP (Protocolo Simple de Administración de Red), y en base a él se diseña un modelo de monitoreo inteligente de red para la prueba del protocolo de Internet (IP) y se desarrolla un sistema de monitoreo de red. En este artículo se explica la propuesta de un "…sistema que realiza el monitoreo del equipo de red, rendimiento y las fallas en redes. El sistema de monitoreo de red realiza consultas remotas en tiempo real, alarmas de fallas, consejos de mantenimiento de equipos de red. El sistema descubre los problemas existentes en la red durante el monitoreo en tiempo real, y proporciona una referencia de decisión para que los administradores de redes encuentren la solución a problemas y garanticen la seguridad y la estabilidad de la red."

Según Francisco Javier Palazón [2], 2018, "Afirma que gracias a los sistemas de monitorización cloud, las empresas efectúan un seguimiento cómodo y exhaustivo de cada uno de los elementos monitorizados ofreciendo un mejor nivel de servicio, productividad y rendimiento; y con la ventaja de hacerlo bajo la fórmula 'as a service'. Los sistemas de monitorización cloud desempeñan un papel importante en la gestión de las infraestructuras TI de las empresas,

en especial cuando hablamos de la nube informática. Al ser servicios de monitorización cloud, la ventaja para las empresas es que éstas contratan un servicio para gestionar uno o varios elementos (red, aplicaciones, almacenamiento…) con la ventaja de que se reducen los costes y el impacto en la propia infraestructura del cliente es mínimo. En lo referente a su funcionamiento, estos sistemas de monitorización cloud han sido creados para vigilar y llevar un seguimiento exhaustivo de cada uno de los componentes elegidos."

Según Walter Goralski [3], 2017, "Expresa que los estándares de gestión de red, funcionan mediante el modelo agente / administrador, que es esencialmente la idea del modelo cliente / servidor ampliado a la gestión de la red. Un agente es un software que se ejecuta en todos los dispositivos administrables de la red. Un administrador es solo una consola de administración en el NOC (Centro de Operaciones de Redes) que ejecuta el software de gestión de red. El modelo del cliente / servidor tradicional es que en una situación de gestión de red, hay muchos servidores (agentes) y, en general, solo unos pocos clientes (gestión consolas). El administrador que se ejecuta en la estación de administración de red (o cualquier configuración de host, para ejecutarlo) envía comandos al software del agente en el dispositivo administrado usando un protocolo de gestión de red que tanto el administrador como el agente entienden. El agente responde y luego espera (o "escucha") un comando adicional, y así sucesivamente. La orden puede ser generada por el software administrador periódicamente, sin intervención humana, y los resultados almacenados en una base de datos de la consola del administrador para informes futuros o de referencia."

Según Gerardo Junco Romero y Sonia Rabelo Padua [4], 2018, "La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico. Mediante SNMP, se define una técnica que es utilizada para obtener estadísticas sobre

la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido."

Según Sara C. Cuchala [5], 2016, "Desde el momento en que las redes se consideran cada vez más una parte esencial y estratégica de las empresas, industrias u otros tipos de instituciones y como resultado de las cada vez mayores dimensiones que están adoptando, resulta más importante su control y gestión con el fin de obtener la mejor calidad de servicio posible. Mediante el uso de un sistema de gestión de red se conseguirá prestar un mejor servicio a los diferentes usuarios de la red del Gobierno Provincial de Imbabura y facilitar la gestión para el administrador de la red de datos de tal manera que exista mayor eficiencia en su trabajo, y por ende se brindará un mejor servicio a la ciudadanía."

Según Sihyung Lee, Kyriaki Levanti y Hyong S. Kim [6], 2014, "El monitoreo de red guía a los operadores de red a comprender el comportamiento actual de una red. Por lo tanto, un monitoreo preciso y eficiente es vital para asegurar que la red opera de acuerdo con el comportamiento deseado para luego solucionar cualquier desviación. Sin embargo, la práctica actual de monitoreo de red depende en gran medida de las operaciones manuales, así las empresas gastan una parte significativa de sus presupuestos en la fuerza laboral que monitorear sus redes. Analizaron las actuales tecnologías de monitoreo de redes, identificaron problemas abiertos, para sugerir futuras direcciones. El primer análisis evaluó qué tan bien se integran las tecnologías presentes con todo el ciclo de operaciones de gestión de red: diseño, implementación y supervisión. Los operadores de red primero diseñaron configuraciones de red, luego desplegaron el nuevo diseño y finalmente supervisaron continuamente el comportamiento de la red. La eficiencia de este ciclo puede ser mejorado en gran medida por la implementación automatizada de configuraciones pre-diseñadas, en respuesta a cambios en el comportamiento de la red monitoreada."

Según Arman Roohi, Khashayar Raeisifard y Suhaimi Ibrahim [7], 2014, “En el enfoque de monitoreo SNMP, los agentes enviarán una información a la estación de gestión de red a través de informes de eventos de sondeo. El sondeo es una actividad en la que hay interacción entre los agentes y la estación de gestión utilizando la solicitud y método de respuesta. El enfoque de monitoreo en tiempo real se define como un acuerdo entre los agentes y la estación de gestión en la que en este tipo de acuerdo los agentes enviarán periódicamente la información a la estación de gestión sin peticiones a la estación. En una organización, el estado y el comportamiento son el fin del sistema que será considerado como trabajo de monitoreo para la información del MIB. El tipo de datos que se utiliza en el monitoreo es más importante que el diseño de red. Dinámico: como paquetes, elementos de red. Estadístico: información dinámica como el promedio de paquetes transmitidos por unidad.”

1.4 OBJETIVOS DE LA INVESTIGACION

1.4.1 OBJETIVO GENERAL

Implementar un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basado en software libre para una empresa e-Commerce.

1.4.2 OBJETIVOS ESPECIFICOS

a.- Analizar y comparar los diferentes sistemas de monitoreo de dispositivos de comunicación y usuarios finales.

b.- Analizar el protocolo SNMP y elaborar un prototipo de sistema de monitoreo de dispositivos de comunicación y usuarios finales aplicado a una empresa e-Commerce.

c.- Implementar el prototipo propuesto para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP aplicado a una empresa e-Commerce usando software libre.

1.5 HIPOTESIS

1.5.1 HIPOTESIS GENERAL

Utilizando el protocolo SNMP se implementará un prototipo de monitoreo de dispositivos de comunicación y usuarios finales basado en software libre para una empresa e-Commerce.

1.5.2 HIPOTESIS ESPECÍFICAS

a.- Analizando y comparando los diferentes sistemas de monitoreo de los dispositivos de comunicación y usuarios finales se podrá proponer nuevas soluciones personalizadas.

b.- Analizando el protocolo SNMP se podrá implementar un prototipo de sistema de monitoreo de dispositivos de comunicación y usuarios finales aplicado a una empresa e-Commerce.

c.- Es posible implementar el prototipo propuesto para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP aplicado a una empresa e-Commerce usando software libre.

1.6 METODOLOGÍA

Para el desarrollo del presente trabajo de investigación la metodología utilizada consta de tres partes: la recopilación de la documentación técnica para el análisis de los diferentes sistemas de monitoreo de redes de datos, la identificación de una empresa que brinde servicios por Internet en la que se propone una arquitectura de monitoreo y la implementación de un prototipo de sistema de monitoreo propuesto.

La propuesta planteada para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP ha sido aplicada a una empresa e-Commerce usando software libre.

1.7 CONTENIDO DE LA TESIS

La presente tesis está conformada por 5 capítulos. En el capítulo 1, denominado Objetivos de la tesis, contiene la introducción, justificación de la investigación, estado del arte, los objetivos generales y específicos de la tesis, así como sus hipótesis. En el capítulo 2, denominado el Marco teórico, contiene los fundamentos teóricos en que se basa la tesis. En el capítulo 3, denominado Propuesta de la tesis, contiene la descripción del prototipo que se propone en la tesis, así como su emulación. En el capítulo 4, denominado Resultados, se explica los resultados de la implementación del prototipo. En el capítulo 5, denominado Conclusiones y Recomendaciones, se indican las conclusiones y recomendaciones de la tesis. Finalmente, se adjunta la bibliografía utilizada en la tesis y anexos donde se detallan los principales procedimientos en la implementación del prototipo.

CAPÍTULO II

MARCO TEÓRICO

2.1 INTRODUCCIÓN

Dada la complejidad de un entorno informático de red, es necesario supervisar y gestionar de manera centralizada los componentes de hardware, conmutadores, routers, como los componentes de software, bases de datos, servidores web, servicios de red. Este desafío, es posible si se utilizan protocolos normalizados, como SNMP.

Una buena gestión de la red de telecomunicaciones contribuye a una eficiente producción en cualquier empresa, independiente del rubro; aun cuando los costos asociados para la implementación de una solución adecuada son elevados, debería estar acorde con los riesgos de pérdida de actividad y por indisponibilidad del servicio [8]. Sin embargo, es posible a través del software libre brindar una solución a bajo costo que permita monitorear el activo de la empresa y permitir la continuidad del negocio, evitando pérdidas económicas significativas.

SNMP (Simple Network Management Protocol) es el protocolo elemental que garantiza el transporte entre equipos supervisados y administrados, además de la consola de administración. El protocolo fue desarrollado para administrar nodos, servidores, estaciones de trabajo, routers, switches y dispositivos de seguridad en una red IP. SNMP es el protocolo de la capa de aplicación que proporciona el intercambio de información entre dispositivos de red.

SNMP está basado en administradores NMS (Network Management Systems), agentes que son los nodos administrados, y las MIB (Management Information Bases) que son las bases de información de administración. El protocolo SNMP se encapsula en UDP (User Datagram Protocol) y hace uso de los puertos 161 y 162 [9].

En esta tesis se analiza la gestión de una red de telecomunicaciones de una empresa relacionada con el comercio por internet y se propone un prototipo para monitorear los dispositivos de comunicación y usuarios finales basados en software libre en este tipo de empresa e-Commerce.

2.2 IMPORTANCIA DE LA GESTIÓN DE REDES DE DATOS

Toda organización hoy en día debe contar con elementos que permitan medir, mantener y mejorar los procesos informáticos, lo comúnmente conocido como “Calidad de Servicio” (*Quality of Service*-QoS), término utilizado para asegurar la continuidad de los servicios ofrecidos en todas las áreas funcionales dentro de la organización.

Cada área de la empresa tiene varios retos a nivel de comunicaciones, almacenamiento y seguridad, que se ponen de manifiesto al momento de configurar y mantener el equipamiento informático que contienen todas las operaciones. Por ello, es fundamental la gestión de red para garantizar estos procesos y la calidad en los servicios.

Existe una gran diversidad de sistemas heterogéneos que requiere la existencia de un marco de elementos (protocolos, estándares, entre otros) que permitan el control permanente de la red, situación que motivó el desarrollo del protocolo SNMP, y en conjunto con otros protocolos de TCP/IP, brindan una gestión de red consolidada y actual, en materia de protocolos de gestión [10].

2.3 MODELOS DE LAS REDES DE DATOS

Para entender el funcionamiento de una red de datos se debe analizar el modelo de referencia OSI y la arquitectura TCP/IP, ambos conceptos facilitan la interconectividad de cualquier tipo de red, independiente de la tecnología que se use, cumpliendo las recomendaciones que se indiquen.

2.3.1 MODELOS OSI

A inicios de los años ochenta los fabricantes informáticos importantes de la época se reunieron para recopilar y unificar en lo posible, la mayor cantidad

de información, acerca de cómo poder integrar sus productos, hasta ese entonces no compatibles y exclusivos para cada uno. Como resultado del acuerdo emerge el modelo de referencia OSI, que cumple con los parámetros comunes de hardware y software haciendo factible la integración multifabricante [11].

El modelo de referencia OSI (modelo abierto de interconexión de sistemas) organiza la red en diferentes capas con la finalidad de que cada desarrollador labore precisamente en su área sin tener que depender de otras áreas. En la figura 2.1, se muestra las siete capas del modelo OSI: Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física.

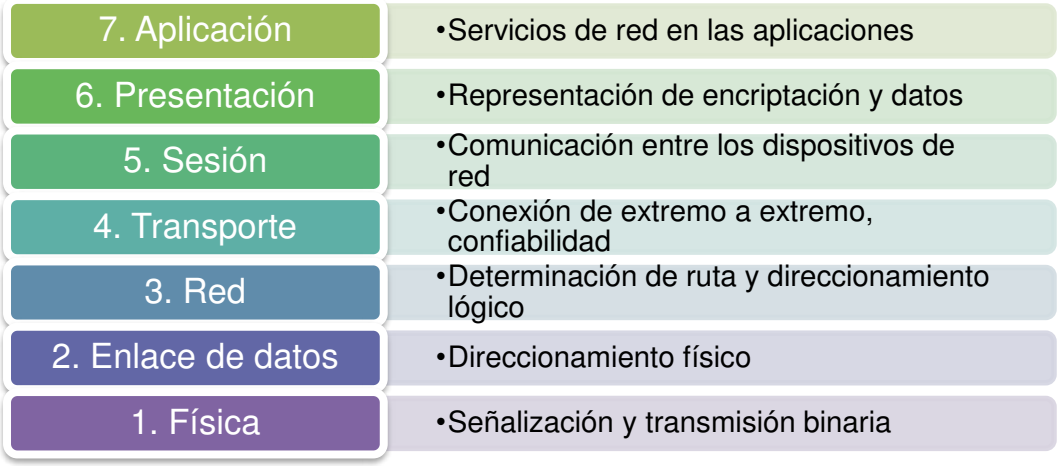


Figura 2.1 Modelo OSI [Ariganello E., 2016, Las siete capas del modelo OSI, Recuperado: Redes Cisco – Guía de estudio para la certificación CCNA Routing y Switching]

El programador crea una determinada aplicación y no considera el medio por el que se trasladan los datos, de la misma manera el especialista de comunicaciones provee el medio sin importarle el tipo de datos que transportará.

La ***capa de aplicación*** al ser la capa de nivel superior del modelo de referencia OSI, no comparte servicio a otra capa. Algunos protocolos de esta capa permiten el manejo de correo electrónico, y acceso remoto.

La ***capa presentación*** garantiza que los datos enviados desde la capa de aplicación del sistema origen sean leídos por la capa de aplicación del sistema destino. Por ejemplo, JPEG y GIF (formatos de imágenes), que se

observan en las páginas web, aseguran que los navegadores web muestren las imágenes, independientemente del sistema operativo utilizado.

La ***capa de sesión*** establece, administra y concluye las comunicaciones entre entidades de la capa de presentación. Por ejemplo, su función es la coordinación entre un servidor y un cliente de base de datos.

La ***capa de transporte***, encargada fundamentalmente de la comunicación entre procesos, el control de flujo y la corrección de errores. En la cabecera, los datos son divididos en segmentos, identificados con un número denominado puerto, que distingue la aplicación de origen.

La ***capa de red*** realiza el direccionamiento lógico de manera jerárquica, selecciona la mejor ruta destino a través del uso de tablas de enrutamiento en las cuales están inmersos los protocolos de enrutamiento dinámicoso o estáticos.

La capa de ***enlace de datos*** proporciona las comunicaciones entre nodos de un mismo enlace, transformando las unidades de voltios en tramas y las unidades de tramas en voltios.

La ***capa física*** es la encarga de los medios, conectores, radiofrecuencia, especificaciones eléctricas, lumínicas, y de la codificación. Los bits se transforman en pulsos eléctricos, luz o radiofrecuencia para ser enviados de acuerdo al medio en que se propaguen.

Principales características del modelo de referencia OSI [11]:

- Brinda entendimiento de cómo operan los dispositivos en una red.
- Referencia para crear e implementar esquemas de *internetworking*, estándares de red y dispositivos.
- Disocia la compleja operación de una red en elementos más simples.
- Faculta a los ingenieros centrarse en el diseño y desarrollo de las funciones modulares al ocuparse cada uno de ellos en su área específica.

- Concede la posibilidad de determinar interfaces estándar para compatibilidad “plug and play” e integración multifabricante.

2.3.2 ARQUITECTURA TCP/IP

El origen de la arquitectura TCP/IP se remonta en la década de los 60, cuando el Departamento de Defensa de EE.UU (DoD) requería la transmisión de datos confiables hacia cualquier destino de la red, dando origen a la red ARPANET. A fines de la década de los 70 se propone arquitectura denominada TCP/IP [12], en base a los resultados de experimentos de interconexión para conectar dos nodos distantes.

La arquitectura TCP/IP es el concepto en el que se cimienta Internet y presenta cuatro capas: capa de aplicación, capa de transporte, capa de Internet y capa de acceso de red. En la figura 2.2, se muestra las capas de la arquitectura TCP/IP.

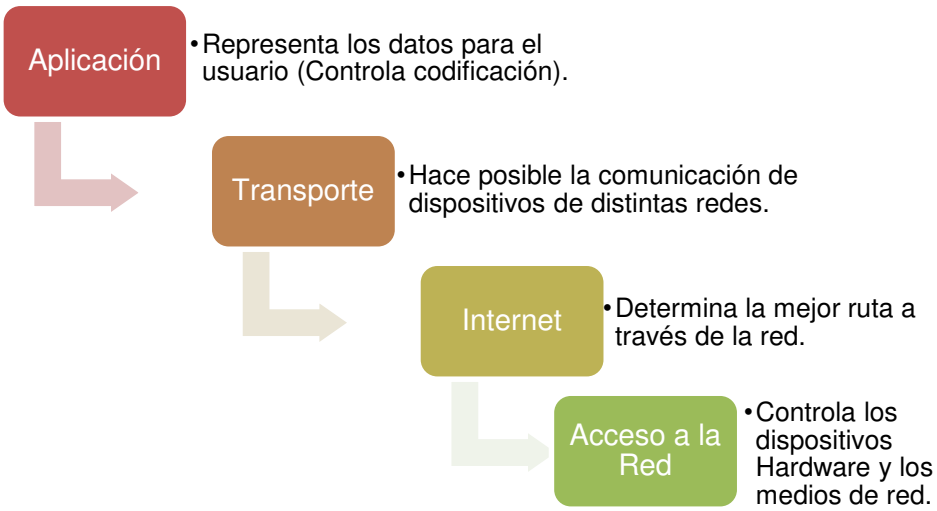


Figura 2.2 Arquitectura TCP/IP [Boronat F., 2013, Recuperado: Direccionamiento e interconexión de redes basado en TCP/IP (IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF)]

La ***capa de aplicación*** es donde se ubican los protocolos: Telnet, FTP, DHCP y SNMP. El protocolo SNMP ofrece una forma de monitorizar, controlar los dispositivos de red, administrar configuraciones, recolectar datos estadísticos, monitorizar el desempeño y seguridad de una red.

La ***capa de transporte*** es la encargada de brindar soporte a la capa de aplicación a través del envío de datos no importando el contenido de éstos. Existen dos protocolos, uno orientado a conexión TCP y otro orientado a

conexión UDP. El protocolo SNMP hace uso del protocolo UDP para que el proceso de gestión sea lo más rápido posible.

La ***capa de Internet*** es la encargada de enrutar los datos por Internet, definiendo la ruta más adecuada según diferentes criterios: ancho de banda, cantidad de saltos, retardo en cada enlace, pesos asignados a cada enlace, entre otros. El principal protocolo de esta capa es IP, en sus dos versiones IPv4 e IPv6.

La ***capa de acceso a la red*** establece las tramas para la conexión de dos nodos ubicados en un enlace, dependiendo de la tecnología del enlace. Una trama muy utilizada en Internet es la trama que corresponde a la tecnología Ethernet.

2.3.3 SOCKET Y LAS APLICACIONES

2.3.3.1 Procesos de comunicación

En una aplicación de red, los programas se ejecutan en múltiples sistemas finales comunicándose entre sí. Estos programas son procesos que se comunican utilizando reglas que se rigen por el sistema operativo final del sistema. Los procesos en dos sistemas finales diferentes se comunican entre sí intercambiando mensajes a través de la red informática. Un proceso de envío crea y envía mensajes a la red; en una recepción el proceso recibe estos mensajes y posiblemente responde enviando mensajes de vuelta [13].

2.3.3.2 Programación Socket

Una aplicación de red típica consiste en un par de programas, un programa cliente y un programa servidor, que residen en dos extremos diferentes (sistemas). Cuando estos dos programas se ejecutan, se crean un proceso de cliente y un proceso de servidor, y estos procesos se comunican entre sí leyendo y escribiendo en sockets. El término socket hace referencia a una interfaz de programación de aplicaciones (API) orientado a los protocolos de Internet del modelo TCP/IP. Los sockets de Internet permiten la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos adecuados.

Actualmente, toda implementación se especificada en un protocolo estándar, como las recomendaciones RFC o algún otro estándar, por ello esta aplicación a veces se denomina "abierta", ya que todos conocen las reglas que especifican su funcionamiento.

Para la implementación, los programas cliente y servidor deben cumplir con las reglas dictadas por las RFC. Si el desarrollador escribe el código para el programa cliente y otro lo hace para el programa del servidor, y ambos siguen cuidadosamente las reglas de las RFC, entonces los dos programas podrán interoperar.

Durante la fase de desarrollo, una de las primeras decisiones que debe tomar el desarrollador es si la aplicación debe ejecutar sobre TCP o sobre UDP.

El flujo de los procesos entre el cliente y el servidor ejecutándose sobre UDP, cuando se usa aplicaciones basadas en SNMP es el siguiente:

En el cliente y en el servidor se crean sockets; el datagrama creado con una IP del cliente y puerto=x es enviado vía socket del cliente al servidor; en el servidor se lee el segmento UDP recibido por el socket del servidor, luego en el servidor se escribe la respuesta al socket del servidor especificando la dirección del cliente así como el número de puerto y es enviado al cliente.

En el cliente se lee el datagrama recibido por el socket cliente culminándose de esta manera con el cierre del socket cliente.

Cuando la aplicación se ejecuta sobre TCP garantiza que el proceso del servidor recibirá (a través del socket de conexión) cada byte en el pedido enviado.

En la figura 2.3 se muestra el proceso entre cliente / servidor haciendo uso de TCP en el cual no solo recibe bytes sino también envía bytes a su conexión [13].

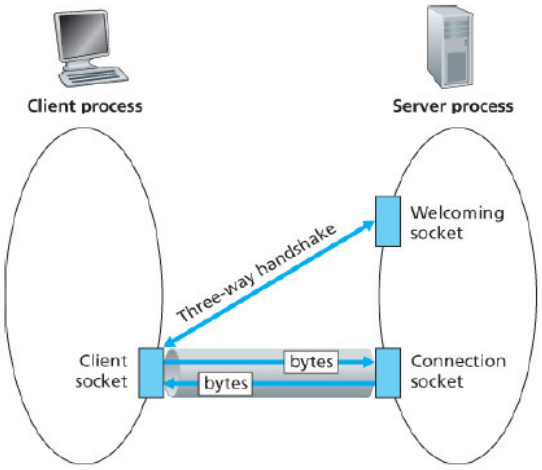


Figura 2.3 El proceso TCP Server tiene dos sockets
[Kurose J., 2017, Recuperado: Computer Networking]

2.3.3.3 Multiplexación y Demultiplexación

Los procesos de multiplexación y demultiplexación, en redes de datos, se emplean en la capa de transporte de la arquitectura TCP/IP, modelo OSI y permite que varias aplicaciones, por ejemplo, relacionados con la gestión de red, pueden ser enviados o recibidos en simultaneo sin ningún tipo de interferencia. Esto se logra asociando a cada aplicación cliente/servidor un par de socket diferentes (número de puerto de la aplicación y dirección IP del host que contiene la aplicación) [14].

2.3.3.4 Transporte sin conexión: UDP

En la transmisión de datos, el protocolo UDP es comúnmente utilizado por un gran número de aplicaciones debido a su mecanismo simple, pequeño retardo de transmisión y alta eficiencia de transmisión [15].

El protocolo de transporte de nivel de aplicación recomendado, es el protocolo de transporte de datos UDP, cuya función principal es transferir datos entre las aplicaciones de una red informática incluyendo sistemas de videoconferencia en línea por ejemplo, que incluyen gran cantidad de aplicaciones de red del modelo cliente / servidor en la que la transmisión y recepción de datos antes de enviar, no establece una conexión, permitiendo así que una máquina pueda dar servicio a múltiples clientes, es decir, un dispositivo terminal puede cumplir la función de cliente y servidor dependiendo del software de configuración [15].

SNMP utiliza el protocolo de transporte UDP. Para enviar un mensaje, una entidad SNMP serializa un mensaje SNMP y lo envía a través de un datagrama UDP a la dirección de la entidad que recibe. Los agentes SNMP escuchan por el puerto 161.

En la figura 2.4 se muestra el transporte de un mensaje SNMP y los protocolos de cada capa involucrada en el proceso.

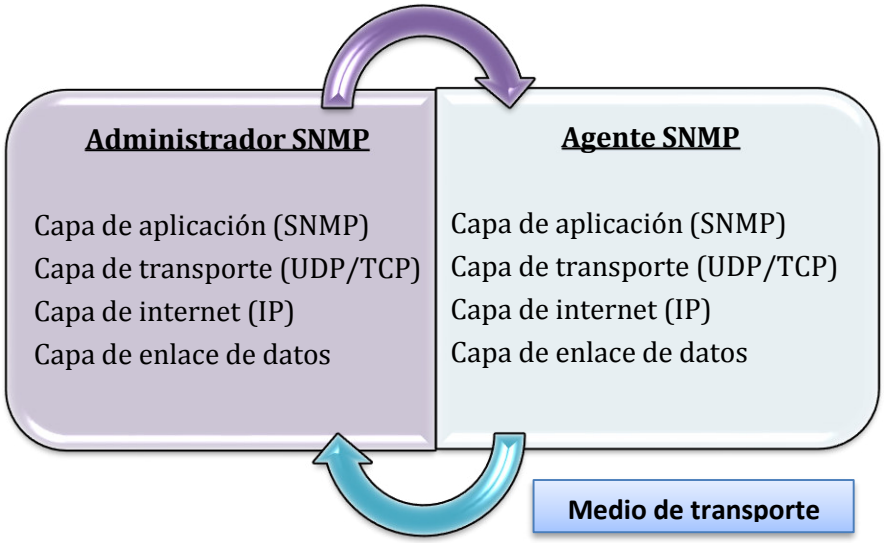


Figura 2.4 Transporte de un mensaje SNMP [Abdullah MK. alt, 2007, Recuperado: Multiplexación por división en ciclo de trabajo (DCDM): una novedosa y económica técnica de multiplexación óptica y demultiplexación eléctrica para redes de fibra óptica de alta velocidad]

2.4 MODELO CLIENTE SERVIDOR

El modelo cliente servidor ha contribuido en desarrollar el uso de los datos a través de los servicios de los protocolos que forman parte de los modelos referenciales más importantes como son TCP/IP y OSI. Este modelo pone en práctica la definición de servicio y la interacción de protocolos donde la comunicación se establece entre un proceso de servidor y un proceso de cliente [16].

El proceso de cliente faculta al usuario formular los requerimientos y pasarlos al servidor, esto se conoce con el término *front-end*. El cliente usualmente administra todas las funciones que implican manipular y desplegar los datos, por ende están desarrollados en plataformas que hacen uso de interfaces gráficas de usuario (GUI), que permiten además, acceder a los servicios

distribuidos en cualquier parte de la red. El servidor es el proceso que atiende a múltiples clientes que realizan peticiones de algún recurso administrado por el mismo. A este proceso de servidor se le atribuye el término *back-end*. Normalmente el servidor, administra las funciones relacionadas con las reglas del negocio y los recursos de datos [17].

En la figura 2.5, se muestra un sistema distribuido; cada máquina puede cumplir el rol de servidor para algunas tareas y el rol de cliente para otras.

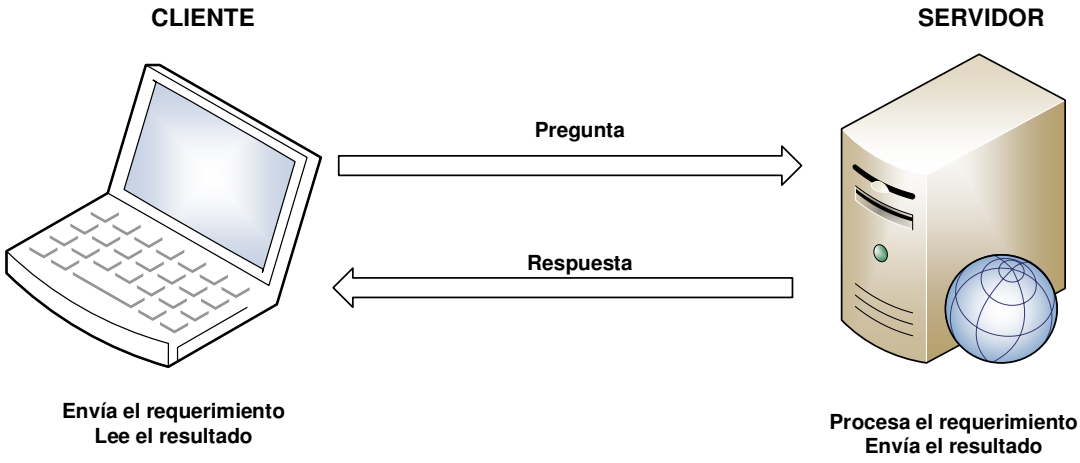


Figura 2.5 Modelo Cliente/Servidor [Serain D., 1995, Cliente / servidor: ¿Por qué? ¿Qué? ¿Cómo?]

2.5 MODELO DE GESTIÓN DE REDES DE DATOS

La gestión de la red se refiere a la supervisión, organización y control de los servicios de comunicación de red, así como el estado de los dispositivos de red. El objetivo es garantizar que la red informática tenga un funcionamiento normal.

La gestión de recursos puede ser asistido mediante el uso de un marco de gestión de red. OSI Network Management Model (NMM) es el modelo estándar y proporciona un marco conceptual para la organización de una diversa gama de recursos de red. NMM OSI cumple un rol importante dentro de grandes redes empresariales centradas en la capacidad y gestión del rendimiento [18].

La OSI NMM define un concepto modelo para la gestión de todas las "entidades" de comunicación dentro de una red. Hay tres componentes

básicos que comprenden los elementos de la arquitectura de gestión para soportar una implementación exitosa de la NMM OSI [18]:

a.- Un componente funcional involucrado con las diversas actividades realizadas en apoyo de la administración de la red.

b.- Un componente de comunicación que se centra en cómo se intercambia la información entre los sistemas gestionados.

c.- Un componente de información involucrado con cinco grandes áreas funcionales: falla, configuración, contabilidad, pronóstico y/o estadística de los eventos. Rendimiento y gestión de seguridad (FCAPS) en gestión de TI que facilitan el rápido y consistente progreso dentro de las áreas individuales de cada categoría [18]:

c.1. La gestión de fallos (F) es un evento que tiene un significado negativo. La gestión está diseñada para detectar, reconocer, aislar, corregir y registrar las fallas que ocurren en la red. Esta función utiliza el análisis de tendencias para predecir el error con la intención de que la red se encuentre siempre disponible y de esta manera mantener la red en funcionamiento.

c.2. La gestión de la configuración (C) se refiere al monitoreo de sistemas de red y sistema de información de configuración; por lo tanto, los efectos en el funcionamiento de la red con varias versiones de elementos de hardware y software pueden ser rastreados y gestionados.

c.3. La gestión contable (A) está involucrada con recopilación de estadísticas de uso de los usuarios. Estas estadísticas de los sistemas de red pueden ser reguladas, lo que puede minimizar las dificultades en la red y maximizar la equidad de acceso en la red para todos los usuarios.

c.4. La gestión del rendimiento (P) determina la eficiencia de la red actual, al inicio relacionado con las inversiones iniciales para instalar

la red. El rendimiento de la red se manifiesta a través del porcentaje de la utilización, rendimiento, tasas de error y tiempo de respuesta. Recopilando y analizando datos del rendimiento de la salud de la red que puede ser monitoreado a través del análisis de tendencias que pueden indicar capacidad y problemas de fiabilidad, para determinar si un problema particular de la red es digno de atención.

c.5. La gestión de la seguridad (S) es el proceso de control de acceso a activos en la red. Puede identificar recursos sensibles de la red y determinar las asignaciones de estos recursos y conjuntos de usuarios. Este proceso también controla los puntos de acceso de los recursos sensibles de la red y registra cualquier acceso inapropiado.

Usando FCAPS es posible definir y por lo tanto administrar la tecnología de la información (TI) de la infraestructura de una organización [18].

La tarea de monitoreo de la red se vuelve tediosa al aumentar el tamaño, la heterogeneidad y la complejidad de la red. Las soluciones de gestión y supervisión de red disponibles no solo son costosas, sino que también son difíciles de utilizar, configurar y mantener.

La localización manual de un dispositivo defectuoso en la gran red compleja es muy complicada y consume tiempo para los administradores de red.

Por lo tanto, es necesario contar con un sistema automatizado en el que se informe al administrador de la red el tipo de error y su ubicación, tan pronto como surja.

El presente proyecto de tesis trata de la implementación de un prototipo de monitoreo de código abierto y su integración inteligente para monitorear dispositivos de red diversos como switches, routers, APs, equipos terminales como teléfonos SIP, impresoras en red, POS y PCs (PC desktop y laptops).

2.6 PROTOCOLO SNMP

El modelo de administración SNMP es el protocolo de la capa de aplicación del modelo TCP/IP que posibilita el intercambio de información entre dispositivos de red; es un protocolo estándar para la red de computadoras. La función básica de SNMP es monitorear el rendimiento, recuperar fallas y configurar los equipos de la red, entre otros [19].

La gestión de la red IP utilizando el protocolo SNMP se centra principalmente en obtener algunas variables de los objetos gestionados que describen la configuración del sistema.

Las variables que se encuentran en la base de información de administración son muy simples y no se pueden heredar. Cuando se necesita administrar nodos de red cada vez más complejos, el protocolo SNMP se ve abrumado. En estas circunstancias, adoptar una gestión de red distribuida, orientada a objetos es particularmente importante.

Debido a que la tecnología distribuida orientada a objetos tiene la característica de herencia, puede mejorar la eficiencia del desarrollo, también puede equilibrar la carga del centro de administración de red, porque las funciones de modelado y recolección de datos se distribuyen en cada dominio de administración al mismo tiempo, con buena escalabilidad [19].

2.6.1 Arquitectura

La arquitectura SNMP básica consta de cuatro componentes fundamentales: elementos de red, estaciones de administración de red, protocolo de administración de red y estructura de la información de gestión [20].

2.6.1.1 Elementos de red

Los elementos de red, tienen agentes de administración de red que reciben las consultas y comandos de la administración de red y actúan sobre aquellos que son auténticos. Además, las capas de protocolo en los nodos gestionados contienen instrumentos que permiten recopilar la información de gestión de red.

Los elementos de red incluyen sistemas finales como hosts, estaciones de trabajo, servidores de terminal, impresoras entre otros. También incluyen sistemas intermedios como gateways, routers, bridges, repetidores inteligentes y MAC inteligente; dispositivos de capa, por ejemplo, concentradores de fibra óptica, repetidores y similares [20].

2.6.1.2 Estaciones de administración de red

Las estaciones de administración de redes son utilizadas por el personal de administración de redes para monitorear y controlar la red. Estas estaciones típicamente ejecutan múltiples aplicaciones en las áreas de gestión de fallos, gestión de configuraciones, gestión de la seguridad y gestión del rendimiento. Estas aplicaciones están unidas por medio de una interfaz gráfica de usuario [20].

2.6.1.3 Protocolo de administración de red

Se utiliza para mover la información de administración de red entre los agentes y las estaciones de administración.

El protocolo resuelve los problemas de compatibilidad e interoperabilidad encontrados en redes heterogéneas resultantes de máquinas con diferentes sistemas operativos, tipos aritméticos, ordenación de bytes, conjuntos de caracteres y similares mediante el uso de una sintaxis de transferencia independiente de la máquina para toda la información.

Esta sintaxis de transferencia es un subconjunto bien diseñado del protocolo de nivel de presentación OSI / ISO conocido como Notación de Sintaxis Abstracta Uno (ASN.1) y las Reglas de Codificación Básica (BER) complementarias definidas por las Normas Internacionales 8824 y 8825 [20].

2.6.1.4 La estructura de la información de gestión (SMI)

Especifica las estructuras comunes y el esquema de identificación para la definición de información de gestión. Esto incluye descripciones de información de un objeto, modelo y diferentes tipos de datos genéricos en conjunto utilizados para describir información de administración. El SMI

define la estructura de árbol básica para la MIB y las reglas para crear variables [20].

2.6.2 La base de información de gestión (MIB)

Los documentos MIB describen objetos gestionados incluyendo sus nombres, sintaxis, semántica, acceso y estado. El primer internet estándar MIB define aproximadamente 120 tipos de objetos. El segundo estándar de Internet MIB, define en total 170 tipos de objetos [20]. Los objetos en la MIB se definen utilizando los mecanismos indicados en la Estructura de Información de Gestión (SMI). Este estándar especifica módulos MIB que cumplen con el SMIv2, que se describe en IETF STD 58 (RFC 2578), IETF STD 58 (RFC 2579) y IETF STD 58 (RFC 2580) [21].

El protocolo SNMP tiene cinco tipos de mensaje:

- ✓ Operación Get-Request: el proceso de gestión recupera información del proceso proxy.
- ✓ Operación Get-Next-Request: solicita el siguiente valor en la tabla, y haciendo uso de Get-Request, puede obtener cada valor en tabla.
- ✓ Operación Set-Request: Establece uno o más parámetros de valor para el proceso de proxy.
- ✓ Operación Get-Response: el proceso de proxy responde el mensaje con Get-Request.
- ✓ Operación de trampa: el proceso de proxy se reenvía mensajes, informando al proceso de gestión que algo sucedió [22].

El simple protocolo de administración de red (SNMP) es un estándar de facto en el dominio de gestión de red. Permite un conjunto muy simple de operaciones de gestión de red, la primera versión SNMPv1 fue desarrollada en 1988 por IETF (Grupo de trabajo de ingeniería de internet) [22].

La siguiente versión SNMPv2 mejoró, pero con un problema de seguridad sin resolver. Finalmente, la tercera versión, SNMPv3 hizo frente a ese problema de seguridad [23]. En la figura 2.6, se muestra el formato de mensaje de SNMP.

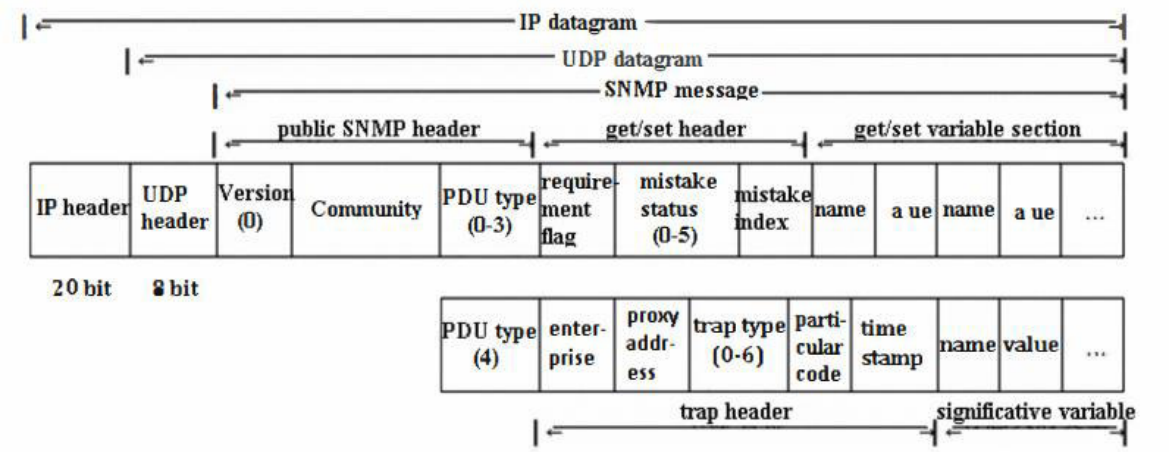


Figura 2.6 Formato de mensaje SNMP [Lu Y. alt, 2010, Recuperado: Investigación sobre la teoría de SNMP y la tecnología de programación SNMP]

En la figura 2.7, se muestra el funcionamiento de SNMP [8].

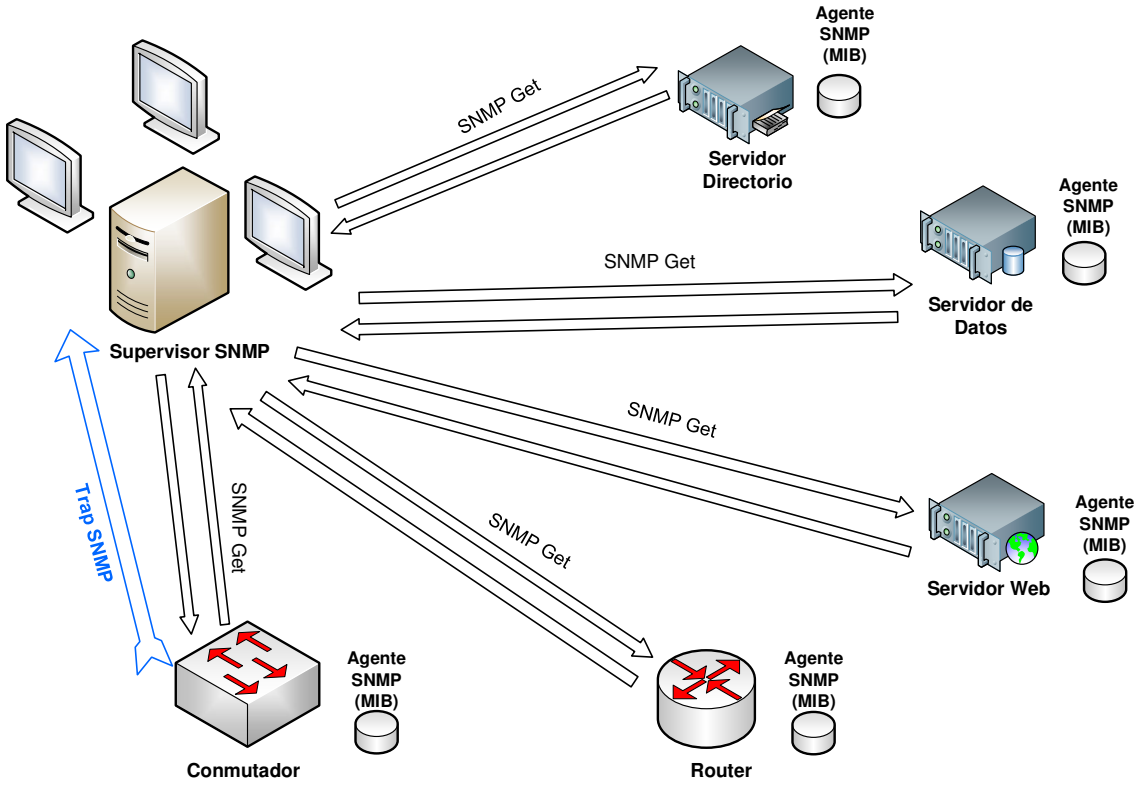


Figura 2.7 Comunicaciones SNMP supervisor – agentes [Dordoigne J., Redes informáticas Nociones Fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IPv6...)]

2.6.3 Solicitudes de comentarios (RFC)

RFC (Request For Comments, Peticiones de comentarios) son un conjunto de documentos referenciales para la comunidad de Internet, estos documentos especifican, describen y asisten en la estandarización, implementación y discusión de los estándares, normas, tecnologías y protocolos relacionados con las redes en general e Internet [24].

En el Anexo II se puede ver una breve lista de las principales RFC utilizados en SNMPv1, SNMPv2 y SNMPv3.

2.7 PLATAFORMA DE GESTIÓN DE REDES DE DATOS

En el ámbito actual de las TICs existen diversas herramientas que ayudan a los especialistas de redes en obtener soluciones completas y fáciles de utilizar, incluso para problemas difíciles de gestión de TI: desde mantener el negocio seguro, hasta garantizar una alta disponibilidad para hacer felices a los usuarios. El objetivo de muchas de estas herramientas consiste en alinear TI con el negocio para que el usuario final no tenga que hacerlo.

2.7.1 SISTEMAS DE MONITOREO – SOFTWARE PROPIETARIO

La Free Software Foundation (FSF Fundación de Software Libre), fundada en 1985, define al software propietario como aquel “que no es libre”, siendo su uso, redistribución o modificación prohibidas, o requieren autorización. Su dominio es privado ya que una determinada persona posee la titularidad de los derechos de autor y por ello exclusividad del acceso al código, fuente del software, utilidad y derecho a copiar, modificar y estudiar el software. El software propietario es imposible de utilizarse en otro hardware o terminal, modificarse y transferirse sin pagar derechos a su creador o desarrollador. Asimismo el adquirir un software propietario implica dependencia total de la empresa desarrolladora, como la firma de contratos por mantenimiento anual, adquisición de nuevas licencias en caso se requiera incrementar la cantidad de sensores, aumentando los costos iniciales. El software propietario está protegido por el sistema copyright, que consiste en asignar y conceder derechos al creador o autor [25]. Entre los sistemas de monitoreo de software propietario se presentan tres.

2.7.1.1 PRTG NETWORK MONITOR

Supervisa toda la infraestructura de TI. Captura tráfico, paquetes, aplicaciones, ancho de banda, servicios en la nube, bases de datos, entornos virtuales, tiempo de actividad, puertos, IP, hardware, seguridad, servicios web, uso de disco, entornos físicos, dispositivos de IoT.

Entre las principales funciones están en que brinda alertas flexibles, muestra diversas interfaces de usuario, mapas y dashboards, monitorización distribuida e informes detallados [26].

2.7.1.2 SOLARWINDS

Identifica rápidamente cambios a nivel de hardware, software registrado a través de la herramienta Server Configuration Monitor.

Entre sus características principales están: Administración de redes, Gestión de sistemas, Seguridad informática, Gestión de base de datos, Servicio de ayuda informática, monitoreo en la nube en tiempo real, monitoreo de aplicaciones e infraestructura, monitoreo de rendimiento web, monitorización y analítica de registros y gestión de registros basados en la nube [27].

2.7.1.3 WHATSUP GOLD – IPSWITCH

Permite medir la disponibilidad y rendimiento de estados activos e inactivos. Obtiene total visibilidad de los estados de los dispositivos, sistemas y aplicaciones de la red, ya sea que estén en la nube o en las instalaciones. Recibe notificaciones proactivas a través de SMS, correo electrónico, web o Slack (herramienta útil para mensajería e intercambio de archivos), sobre los problemas en desarrollo antes de que los usuarios lo informen.

Sus principales características son: descubrimiento y asignación de redes, alerta y monitoreo de redes, generación de informes, tableros y monitoreo en la nube [28].

2.7.2 SISTEMAS DE MONITOREO – SOFTWARE LIBRE

La FSF (FSF Fundación de Software Libre) determina la capacidad de los usuarios para distribuir, estudiar, cambiar, ejecutar y mejorar el software brindado por las comunidades que imparten el software libre, lo que implica ventaja para los usuarios ya que el código fuente ha sido puesta a disposición de los usuarios, siendo posible su adaptación a los cambios del entorno en donde se esté utilizando, satisfaciendo las necesidades peculiares.

La característica más resaltante es que para descargar y utilizar esta clase de software no es necesario realizar pago alguno, es decir, cualquier usuario puede adquirir el código del programa, realizar las adecuaciones y modificaciones para mejorar ciertos requerimientos particulares o generales [25].

Entre los sistemas de monitoreo de software libre se presentan tres.

2.7.2.1 CACTI

Solución completa de gráficos de red, elaborada para utilizar la potencia del almacenamiento de datos y la funcionalidad de gráficos de RRDTool. Cacti proporciona plantillas de gráficas avanzadas, rápido sondeador, métodos de adquisición de datos y funciones de administración de usuarios. Todo, enfocado en una interfaz intuitiva para instalaciones del tamaño de una LAN hasta complejas redes con gran cantidad de dispositivos.

Funciones: Brinda fuentes de datos, gráficos, administración de usuarios y plantillas [29].

2.7.2.2 PANDORA FMS

Software cuya función principal es la monitorización que permite gestionar infraestructura TI. Incluye el equipamiento de la red, servidores de sistemas operativos Windows y Unix, todo tipo de aplicaciones e infraestructura virtualizada. Este software tiene múltiples funcionalidades, lo que lo convierte en un software que cubre los aspectos de monitorización necesarios para su organización [30].

Funciones principales: SLA e informes, control remoto de equipos, monitorización descentralizada, consola visual personalizable, gestión de errores y eventos, alta disponibilidad, capacidad recomendada por servidor, gestión centralizada con políticas de monitorización, actualizaciones automáticas y geolocalización GIS [30].

2.7.2.3 OPENNMS

OpenNMS es una plataforma de código abierto altamente integrada, de nivel de operador, diseñada para crear soluciones de monitoreo de red (gestión de red que determina la disponibilidad de los servicios de red). Es una herramienta diseñada para administrar diferentes dispositivos de red desde un sólo servidor, además de administrar dispositivos que hacen uso de un clúster de servidores. Diferentes herramientas abordan la tarea de monitoreo de diferentes formas, y OpenNMS usa el concepto de "transacciones sintéticas" que intentan imitar la experiencia del usuario. Por ejemplo, para probar si un servidor DNS se está ejecutando, OpenNMS solicitará una búsqueda de DNS desde el dispositivo. OpenNMS es una plataforma de administración, monitorización de servicios y redes para el descubrimiento automático de nodos, notificación de problemas al operador, consolidación de eventos y acción automática. Hay dos distribuciones de OpenNMS: Meridian y Horizon. El uso de Meridian es recomendable para empresas y negocios que buscan estabilidad y soporte a largo plazo. Horizon es el lugar donde la innovación ocurre rápidamente y es ideal para monitorear nuevas tecnologías y ecosistemas de TI. Ambas distribuciones son completamente de código abierto. La plataforma de gestión de red bajo el modelo de Open Source brinda una serie de servicios que se mencionan a continuación [31]:

- **Garantía de servicio**

Detecta las interrupciones del servicio y mide la latencia para la representación gráfica y el umbral a través de encuestas sintéticas. Compatibilidad inmediata con muchas aplicaciones con monitores de servicio configurables. Supervisa remotamente las aplicaciones y servicios desde la perspectiva del usuario [31].

- **Gestión del rendimiento**

Recopila métricas de rendimiento de los agentes estándar de la industria a través de SNMP, JMX, WMI, NRPE, NSClient ++ y XMP simplemente a través de la configuración. Recopila datos de rendimiento de aplicaciones a

través de colectores genéricos personalizables con HTTP, JDBC, XML o JSON [31].

- **Fácil integración**

Utiliza la arquitectura flexible y extensible de OpenNMS para ampliar los marcos de recopilación de datos de rendimiento y sondeo de servicios. Las alarmas en las interfaces y la API ReST ayudan a integrar OpenNMS en su infraestructura existente [31].

- **Evento conducido**

OpenNMS está construido sobre una arquitectura dirigida por eventos. Los eventos se crean a partir de OpenNMS si los servicios, interfaces o nodos se desactivan o se superan los umbrales. Las capturas SNMP y los mensajes de syslog se normalizan en eventos y se pueden correlacionar para crear flujos de trabajo de alarma de alto nivel [31].

- **Descubrimiento de topología**

Descubra topologías de red de capa 2 basadas en información SNMP de estándares de la industria como LLDP, CDP y descubrimiento Bridge-MIB. OpenNMS admite el descubrimiento de topología de enrutamiento de capa 3 basado en OSPF e IS-IS. Las topologías se enriquecen con información de monitoreo [31].

- **Aprovisionamiento**

Descubre la red y sus aplicaciones a través de interfaces manuales, detectadas o controladas por API ReST a través del sistema de aprovisionamiento OpenNMS. Controla la administración de dispositivos con la capacidad de agregar, cambiar y eliminar dispositivos [31]. Entre las últimas innovaciones de la plataforma de monitoreo podemos mencionar: servicio heatmap (para una rápida identificación de problemas, existe un mapa de calor de servicio interactivo permitiendo profundizar rápidamente hasta el origen de un problema), visualización del gráfico estadístico, mapa geográfico, soporte grafana (permite crear cuadros de mando de rendimiento

altamente personalizables e interactivos para una variedad de casos de uso), monitoreo de servicios de negocios, elasticsearch forwarder (envía alarmas unificadas y enriquecidas de OpenNMS a Elasticsearch y visualiza los datos con Kibana) [31].

2.7.2.3.1 Funciones del Software

- ✓ Gestión de eventos y alarmas (Gestión de fallos): Registra todos los eventos ocurridos de la red generando alarmas a los usuarios y al administrador de red [31].
- ✓ Rendimiento y gestión de recolección de datos (Gestión de contabilidad): Mantiene un registro constante de los datos usados por el cliente y permite generar umbrales y alarmas cuando los usuarios rebasen estos límites [31].
- ✓ Integración y gestión de configuración: los tiempos de barrido, mapeado de traps referidos a eventos, alarmas, gestión de MIBs, etc., son incluídos en las configuraciones [31].

2.7.2.3.2 Servicios

Los servicios que puede detectar OpenNMS en una red son los siguientes [31]: Citrix, DHCP, DNS, FTP, HTTP, HTTPS, ICMP, IMAP, JBOSS, JDBC, JSR160, K5, LDAP, Microsoft Exchange, MX4J, NSClient (Agente Nagios), NRPE (Nagios Remote Plugin Executor), NTP, POP3, SMB, SMTP, SNMP, SSH, TCP, Servicios de windows (basados en SNMP)

2.7.2.3.3 Beneficios del sistema de monitoreo de red OpenNMS

- Código abierto (licencia GPL)
- Descubre host en diferentes subredes
- Importa archivos de otras fuentes
- Realiza el diagrama de la topología de la red
- En cada host encontrado se analiza los servicios disponibles
- Obtiene estadísticas de eventos ocurridos, mediante gráficas, discernidos por protocolos
- Gestiona alertas
- Configuración de notificaciones y reportes programados

- Brinda seguridad en la red puesto que maneja protocolos propietarios de encriptación
- Instalación de agentes de supervisión en los clientes para un monitoreo más efectivo
- Aseguramiento de servicio
- Medición del desempeño

Cabe resaltar que estos sistemas de monitoreo son patrocinadas por la ***Free Software Foundation,*** bajo la responsabilidad de la LICENCIA PÚBLICA GENERAL DE GNU [32].

2.7.3 SISTEMAS DE MONITOREO EN LA NUBE

Cada día la tecnología como la conocemos no permanece constante por lo que sufre cambios, mejorías, innovaciones por lo que el tradicional sistema de monitoreo basado en software alojado en dispositivos de comunicación como servidores físicos ha evolucionado al grado de tener hoy en día sistemas de monitoreo en la nube de la cual podemos mencionar tres:

2.7.3.1 AMAZON CLUODWATCH

Es un servicio de administración y monitoreo creado para operadores de sistemas, desarrolladores, ingenieros de fiabilidad de sitio y gerentes de TI. CloudWatch brinda datos e información procesable para monitorear las aplicaciones, entender cambios de rendimiento que afectan al sistema para luego tomar acciones, optimizar la utilidad de los recursos y conseguir unificación del estado de las operaciones.

El servicio de monitoreo, CloudWatch recopila datos de monitoreo y operaciones en formatos de registros, eventos y métricas, lo que ofrece una vista unificada de los recursos, las aplicaciones y servicios que se ejecutan en servidores locales. Proporciona alarmas de alta resolución, ofrece registros, métricas, acciones automatizadas, resuelve errores y descubre información para optimizar sus aplicaciones y asegurar que se estén ejecutando sin problemas [33].

2.7.3.2 ZOHO

Ofrece mesa de ayuda hasta operaciones optimizadas, que ayudan a alinear TI con el negocio. Entre sus principales características podemos mencionar: administra tickets de TI, administra cambios y permite ser activado desde una única consola para garantizar la disponibilidad y mantener el funcionamiento del negocio [34].

2.7.3.3 IBM (Gestión de eventos en la nube)

Identifica, notifica y resuelve incidentes críticos de manera rápida [35]. La gestión de eventos en la nube correlaciona automáticamente los eventos con vistas de incidentes priorizadas. También notifica a la persona correcta en el momento adecuado, con notificaciones integradas y automatizadas. Esto inicia una respuesta rápida y mantiene a todos sincronizados. Para resolver incidentes rápidamente, incluso combina runbooks en contexto con eventos [35].

2.8 GESTIÓN DE RED DE DATOS DE UNA EMPRESA E-COMMERCE

La revisión y análisis continuo de los dispositivos de interconexión de la red y los computadores personales de una organización, describen perfectamente la acción de monitorear redes y sistemas para evitar fallos y pequeños errores hasta catastróficos; esta actividad crea informes a través de notificaciones para los administradores de redes, además crean reportes para solucionar situaciones críticas mostradas en la monitorización de la red de datos.

Todo departamento de informática debe tener un sistema de monitorización, para conocer el desempeño y optimizar los recursos tecnológicos de la organización, como el ancho de banda, tiempos de respuesta de paquetes de datos, manejo de las direcciones IP, acceso a servidores locales, uso de memoria RAM y de CPU de los dispositivos, actualizaciones de sistemas, velocidad de ventiladores entre otros [36].

2.8.1 Beneficios de usar un sistema de monitorización

a.- Mantiene la credibilidad: un excelente sistema de monitorización garantiza el correcto funcionamiento de la organización y/o empresa e-commerce.

b.- Incremento de la eficiencia: administradores del sistema y los usuarios pueden realizar otras actividades ya que el sistema de monitoreo se encarga de avisar y alertar cuando la atención es necesaria.

c.- Reducción de costos: solucionar problemas de forma preventiva, reduce costos ocasionados por equipo de staff, hardware y software.

La gestión de la red haciendo uso de un sistema de monitorización es la solución para mejorar la calidad de los servicios, incrementar el orden y asegurar el éxito tecnológico [36].

"Cada día es mayor el porcentaje de dependencia de negocios y empresas en los sistemas de información y la tecnología. Especialmente esta última se convierte en un habilitador del negocio como tal y soporta su operación, y lo que se busca con el monitoreo es garantizar la disponibilidad de esas soluciones informáticas al servicio de las organizaciones" [36].

2.8.2 Mantener la productividad en la empresa

En general, cualquier organización o empresa e-commerce cuya operación implique procesos de disponibilidad continua (24x7), requiere sistemas de monitoreo. El sector bancario y el de telecomunicaciones son ejemplos comunes de los sectores que requieren de estos sistemas, ya que las empresas necesitan asegurar la disponibilidad y la continuidad del servicio para sus usuarios finales [36].

Otras compañías que necesitan estas soluciones corresponden a aquellas que no cuentan con personal técnico en todas sus sedes para resolver problemas que se presentan. Por ende, un sistema de monitoreo resulta ideal para cualquier empresa que posee sedes remotas y no puede tener personal de operación permanente, pero que sí necesita tener control sobre lo que ocurre en esas locaciones [36].

Una empresa e-commerce que presta servicio continuo al usuario (24x7) con varias sedes remotas, requiere un sistema de monitoreo que le permita conocer el estado de la red LAN-WAN de la empresa brindando información relevante del estado de los dispositivos, tráfico en la red generado por el consumo del ancho de banda realizado por los usuarios finales en las sedes remotas entre otros análisis, que permitan tomar decisiones importantes en el instante en el que ocurran los eventos o sucesos inesperados que interrumpan la continuidad del negocio de la empresa.

2.8.3 Seguridad en la red

2.8.3.1 Protocolo IPsec

Tipo de protocolo que propone el Grupo de trabajo IPSec IETF para proporcionar seguridad de comunicación para la capa IP. En el protocolo de seguridad, se definen los métodos de protección de la comunicación como los parámetros de negociación. Proporciona dos tipos de mecanismos de protección de la comunicación: ESP (Carga de seguridad de encapsulación) y AH (autenticación de cabecera). El protocolo IKE es adoptado para realizar los parámetros de seguridad automáticos. En la negociación, los parámetros de seguridad negociados en IKE incluyen algoritmos de encriptación y autenticación, modo de comunicación protegida (modo de transmisión o túnel) y tiempo de vida de la clave. Para paquetes IP, dos modos de encapsulación incluyendo el modo de transferencia y el modo túnel es ofrecido por ESP. En el modo de transmisión, la cabecera IP no ha cambiado, solo los datos de la capa de transporte está encriptado. En modo túnel, todo el paquete de datos IP es encapsulado con una nueva cabecera IP [37].

2.8.3.2 Protocolo SSL

SSL (Secure Sockets Layer) es un conjunto de seguridad de datos de Internet, protocolos desarrollados por la compañía Netscape que ha sido utilizado para la autenticación de identidad y transmisión de datos entre el navegador web y el servidor. El protocolo SSL se puede dividir en dos capas: protocolo SSL Handshake y el protocolo de registro SSL. Protocolo de registro SSL se basa en el protocolo de transporte confiable (como TCP) que

proporciona encapsulación de datos, compresión, cifrado y otros básicos. El protocolo se basa en el protocolo de grabación SSL que se utiliza para la autenticación de identidad, consulta, intercambio de cifrado, clave y algoritmo de cifrado en la transferencia de datos reales [37].

2.8.3.3 Comparaciones entre IPSEC Y SSL VPN

A. Ámbito de aplicación. - En la capa de red, funciona el protocolo IPSec. Resguarda los datos de transmisión de comunicación para ambos lados, y la aplicación superior es independiente. IPSec VPN es básicamente adecuado para todo tipo de aplicaciones; mientras que el protocolo SSL se encuentra en la capa de socket y está relacionado con la capa de aplicación [37].

B. Complejidad de la operación. - La operación de la VPN IPSec es más complicada en comparación con SSLVPN. El usuario remoto debe instalar un software de cliente específico, en este proceso se debe garantizar que los túneles de seguridad de varios dispositivos de comunicación estén configurados correctamente. SSL VPN no necesita ningún software de cliente especial y ninguna configuración manual. Solo necesita un navegador web; el usuario puede realizar la conexión con el servidor remoto a través de un nombre de usuario, contraseña y URL de puerta de enlace SSL [37].

C. Estrategia de seguridad. -

Autenticación: La autenticación IPSec VPN es más segura. IPSec VPN debe instalarse en el software cliente, lo que hace que los usuarios de equipos remotos estén limitados. La autenticación de la VPN IPSec está directamente relacionada con el equipo, los parámetros de red, la configuración de la política y la dirección IP del dispositivo que utiliza un nombre de usuario, contraseña y cuenta de inicio de sesión para autenticar la seguridad de la conexión remota normal. Por el contrario, los usuarios de SSL-VPN pueden instalarse en lugares públicos para iniciar sesión en la red remota [37].

Encriptación: En IPSec VPN, se adoptan los algoritmos DES de 56 bits, 112 bits y 168 bits, o se utilizan algoritmos de encriptación AES de 192 bits, 256

bits. En el protocolo IPSec VPN, el servidor y el cliente seleccionan el algoritmo de cifrado por SA (Security Association) al inicio de la comunicación. SSL-VPN utiliza un algoritmo de cifrado RC4 de 40 bits o 128 bits, por lo tanto, su seguridad es relativamente más baja que la VPN IPSEC [37].

2.8.3.4 Firewall

Los firewalls son elementos cruciales en la seguridad de la red y se han implementado en la mayoría de empresas e instituciones para asegurar las redes privadas. Su función es examinar cada paquete entrante y saliente y decidir si acepta o desecha el paquete en función de su política [38].

Un firewall es situado en el punto de entrada entre una red privada y el servicio externo de internet ofrecido por un ISP, para que todos los paquetes entrantes y salientes tengan que pasar a través de él. Un paquete puede ser visto como un número finito de campos (dirección IP de origen y destino), el puerto de origen y destino (número y tipo de protocolo). Un firewall mapea cada paquete entrante y saliente y la decisión que toma de acuerdo con su política define qué paquetes son legítimos y son ilegítimos por una secuencia de reglas. Un paquete coincide con una regla si y solo si el paquete cumple el predicado de la regla. El predicado de la última regla en un cortafuego suele ser una tautología para garantizar que cada paquete tiene al menos una regla coincidente en el firewall [39].

Los ataques cibernéticos en dispositivos integrados pueden afectar el acceso a infraestructuras críticas. Por lo tanto, es muy importante proteger estos sistemas de ataques externos mediante la configuración de reglas de firewall en la red. Errores leves en las definiciones de reglas pueden hacer que el tráfico de red malintencionado, no deseado, ingrese a la red o que bloquee el tráfico seguro. Las reglas mal configuradas, pueden dejar puertos abiertos peligrosos que permiten a los intrusos obtener acceso al sistema a través de servicios vulnerables [40].

2.8.4 Concepto de Hosting y Housing

Hosting hace referencia a la instalación de sitios web en un centro de datos. Housing hace referencia a la instalación de un determinado servidor en dicho centro de datos; es decir, el proveedor del servicio de internet (ISP) pone a disposición del cliente la instalación, pero no el propio equipo [41].

2.8.4.1 Servicio hosting

Provee a los clientes un determinado espacio en Internet para que alberguen sus sitios web. Proporciona servidores web, que utilizan conexiones de alta velocidad para prestaciones a nivel de seguridad y conectividad [41].

2.8.4.2 Servicio housing

Es el alquiler de un espacio en un centro de datos, donde los clientes pueden instalar sus propios servidores en un entorno dotado de máxima seguridad y alta velocidad en la conectividad. Los clientes obtienen espacio, potencia eléctrica, servicios de seguridad, refrigeración y conectividad. Los servidores son gestionados por los clientes mas no por la empresa proveedora del servicio [41].

2.8.4.3 Diferencia entre hosting y housing

El housing se centra en el alojamiento físico del propio servidor. Es un servicio bastante demandado por empresas que presentan limitaciones en sus instalaciones, ya sea por razones de seguridad, o porque simplemente no reúnen las condiciones adecuadas para su alojamiento.

El hosting es un servicio de alojamiento virtual, donde los clientes por lo general almacenan sus sitios web, además de archivos e información.

La mayoría de clientes desconocen el modelo del servidor en el que se encuentran alojados sus sitios webs; simplemente acceden a este dispositivo a través de un panel de control. En el caso de que una compañía requiera de una mayor seguridad, mayor capacidad de almacenamiento, como por ejemplo una tienda online con un importante volumen de tráfico, la contratación de un servicio de housing es recomendable [41].

2.8.5 Análisis de la importancia de un sistema de monitoreo en una empresa e-commerce

Consideremos que la empresa e-commerce tiene 3 sedes remotas con infraestructura física en el departamento de Lima y más de 20 sedes remotas en el interior del país (Perú) también con estructura física y cuenta con 250 empleados en la sede principal ubicado en Lima.

Para interconectarse con dos de sus sedes remotas ubicadas en Lima una solución es a través de “VPN Site to Site” o “VPN IPsec tunnel”, otra solución es interconectando una sede remota en Lima a través de un medio diferente como un radio enlace (vía microonda), haciendo uso de una línea de vista proporcionada por dos antenas ubicadas en la sede central y en la sede remota número 3. Las sedes al interior del país de esta empresa e-commerce se interconectan con la sede central a través de VPN SSL. Las sedes remotas, de Lima y el interior del país, deben interconectarse con los servidores de producción, ubicados en la sede central, donde se centra la base de datos de las aplicaciones, para realizar transacciones como facturación electrónica, venta de productos en línea, muestra de catálogos en línea (repositorios de las imágenes se encuentran en los servidores de producción), cierre de ventas a través de un call center propio de la empresa, ubicado en la sede central.

Dado a que la empresa ofrece servicios (24x7), debe garantizar que los dispositivos de comunicación se encuentren operativos sin ningún incidente de fallos, sin afectar sus ventas a través del call center, ventas en línea o ventas manuales, manteniendo el diagnóstico (en tiempo real) del estado de los equipos terminales. El flujo de venta de una sede remota en Lima, se da a través de los equipos terminales como tablets, cuya función principal es realizar ventas rápidas y la conectividad al servicio de internet se realiza a través de la señal WIFI, alimentado por un AP. Otro medio por el que se concreta una venta es haciendo uso del sistema propio de la empresa (versión escritorio y web) mediante las PCs en tiendas. Por ello, es de vital importancia tener el control de los dispositivos de comunicación como el AP y el router por ejemplo, ya que de tener averiado estos equipos dejarían sin

conectividad a la tablet y a las PCs de tiendas, ocasionando pérdidas en las ventas tanto vía online como manual, ambas vías hacen uso de facturación electrónica. En el hipotético caso de que la antena ubicada en la sede central no se encontrara operativa, por problemas físicos del dispositivo de comunicación, dejaría sin conectividad a todos los usuarios administrativos de la sede 3 de la empresa e-commerce, además de dejar sin conectividad a la tienda que se encuentra en esa sucursal.

Con un sistema de monitoreo funcionando en esta red, permitiría al administrador de red identificar a través de las alertas y/o notificaciones el problema en tiempo real y podría optar por soluciones alternas o de contingencia para dar solución a la falta de conectividad con la sede 3 de dicha empresa e-commerce. Por otra parte, el alto uso del servicio de internet, reflejado en el ancho de banda o tráfico generado por los usuarios finales de la empresa e-commerce, genera una elevada latencia o tiempo de respuesta, en la velocidad de navegación de la sede central, afectando directamente a las comunicaciones de los gerentes de la empresa, (evitando que realicen importantes transacciones financieras y cierres de contratos realizados vía videoconferencia) puesto que la conectividad de internet presentará interferencias y/o pérdidas de conectividad, ocasionados por pérdida de paquetes y consecuente la pérdida del servicio de internet y reconexión tardía del servicio.

Sin un sistema de monitoreo, el administrador de la red no podrá conocer que los inconvenientes por intermitencias en el servicio de internet, así como la pérdida de conectividad hacia internet, originado por el uso elevado del ancho de banda por parte del personal administrativo de la sede central; es decir con el sistema de monitoreo de red podría solucionarse a tiempo porque contaría con un reporte, en tiempo real, de lo sucedido haciendo uso del protocolo SNMP, protocolo simple de administración de red. Para analizar la importancia de un sistema de monitoreo en una empresa e-commerce es importante conocer la topología de la red.

En la figura 2.8 se muestra una topología típica de una red de datos de una empresa e-commerce.

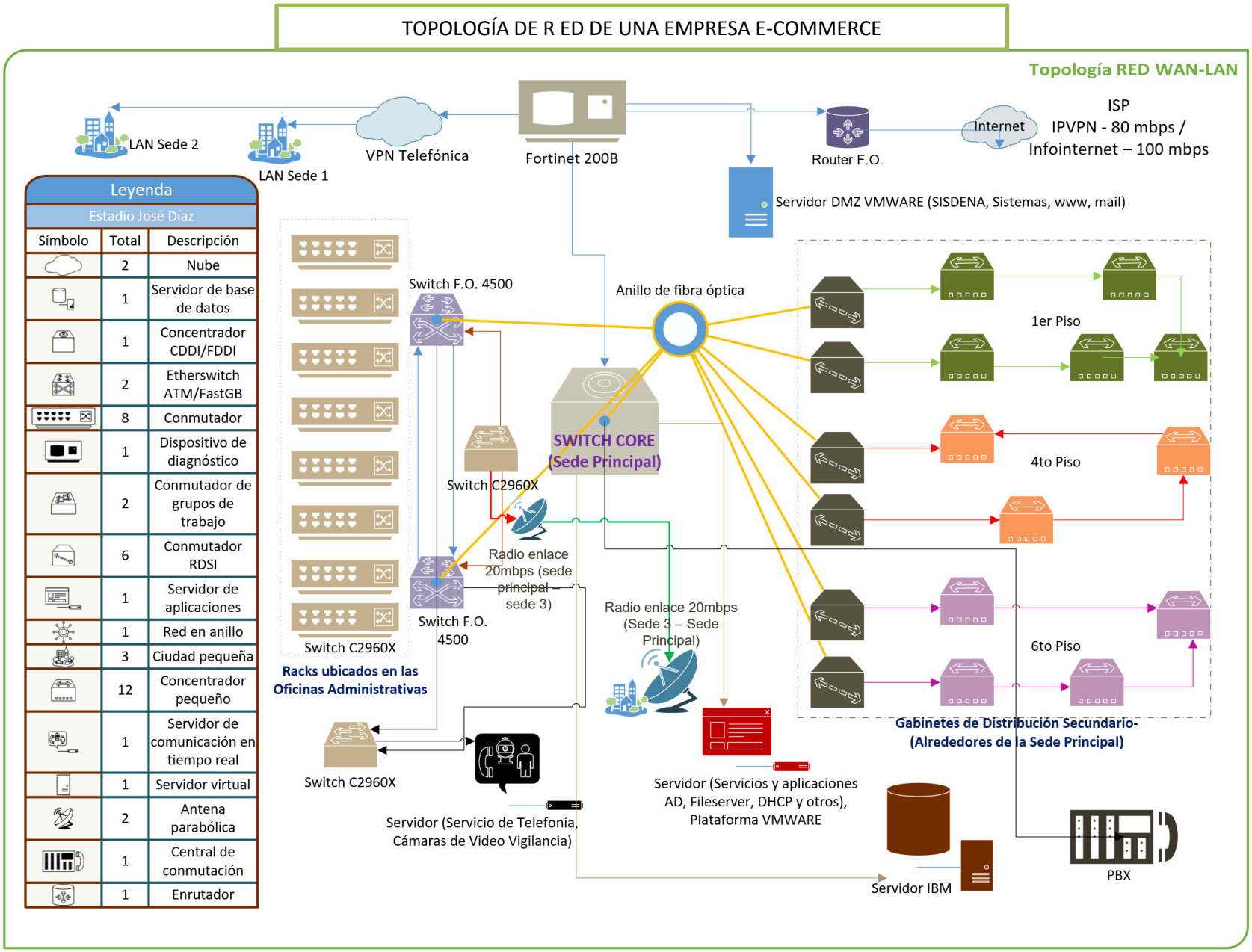


Figura 2.8 Topología de red de una empresa e-commerce [Elaboración propia]

2.9 GESTIÓN Y MONITOREO DE INFORMACIÓN EN REDES CON CONTROL CENTRALIZADO

Como parte de la red global todavía se está utilizando la arquitectura tradicional descentralizada; la descentralización adapta las necesidades del usuario, facilita el reparto de tareas y prolifera la eficacia de las funciones directivas.

La centralización de las aplicaciones y de las bases de datos, fueron provocados por el desarrollo de los mainframes y de las redes terminales, después se retornó a la descentralización con los miniordenadores, producto de la tecnología de los sistemas abiertos.

La última tendencia fue la de controlar los recursos de información de una empresa; el resultado ha sido volver a la centralización, y en otras ocasiones, un desarrollo de estructuras híbridas con componentes centralizados y descentralizados.

En la actualidad, la arquitectura de red tradicional no puede satisfacer todos los requisitos de las nuevas aplicaciones; de acuerdo con los requisitos de la aplicación, los sistemas de red deben ser inteligentes para su adaptación, flexibilidad y optimización.

La aceptación de dispositivos móviles, la diversidad de contenidos, los servicios en la nube y la virtualización de servidores forman parte de las nuevas tecnologías de red que hacen uso de las aplicaciones para mejorar nuestra vida diaria.

En conclusión las futuras redes deberán proporcionar dos funciones: la capacidad de virtualizar una red física y la capacidad de permitir el control independiente de programación para cada partición; estas características son propias de las Redes Definidas por Software o *Software Defined Networking*-SDN [42]. SDN mejora la programación de la red y proporciona una visión global de toda la red al separar el plano de control del plano de datos, esto origina que se distinga la transmisión de datos de las operaciones de control [43].

SDN carece de herramientas de gestión maduras, por lo tanto, un grupo de investigadores de la Universidad de Beijing de Telecomunicaciones decidieron fusionar NMS (el NMS tradicional (Network Management System) adopta SNMP) con SDN y se les ocurrió SDNMP.

Presentaron el diseño de SDNMP, que es un enfoque para la gestión de SDN utilizando NMS tradicionales. Añadieron función de adquisición de datos, procesamiento y almacenamiento de datos; para verificar su enfoque, construyeron e implementaron un prototipo en su propio banco de pruebas.

Al implementar redes y servicios virtuales, los resultados mostraron que SDNMP funciona bien en práctica. Los resultados del experimento también mostraron que SDNMP permite la gestión de redes físicas, virtuales, tabla de flujo y servicios usando SNMP [44].

2.9.1 Redes Definidas por Software

Con el advenimiento de la computación en la nube, se han introducido muchos nuevos conceptos de redes para simplificar la administración de la red y brindar innovación a través de la capacidad de programación de la red. La aparición del paradigma de red definida por software (SDN) es uno de estos conceptos adoptados en el modelo de nube para eliminar los procesos de mantenimiento de la infraestructura de la red y garantizar una gestión fácil. De esta manera, SDN ofrece un rendimiento en tiempo real y responde a los requisitos de alta disponibilidad [45].

Las redes definidas por software (*Software Defined Networking*-SDN) están facilitando a las organizaciones el despliegue de aplicaciones ofreciendo la capacidad de escalar los recursos de la red. SDN administra redes que separa el plano de control del plano de datos para una mejor experiencia de usuario; esta segmentación de la red ofrece numerosos beneficios en términos de flexibilidad y capacidad de control de la red, por un lado, permite combinar las ventajas de la virtualización de sistemas y computación en la nube, por otro, crear inteligencia centralizada que permita tener una visibilidad clara en la red para facilitar la administración y el mantenimiento de la red [45].

En la figura 2.9 se muestra la topología de una estructura de red convencional donde el plano de control y de datos se encuentran vinculados en cada dispositivo lo que resulta complejo a la hora de implementar una nueva solución solicitado por el cliente. También se observa la topología de red de una estructura basada en SDN donde el plano de control y de datos se encuentran separados para brindar una mejor gestión y flexibilidad a una determinada red de datos.

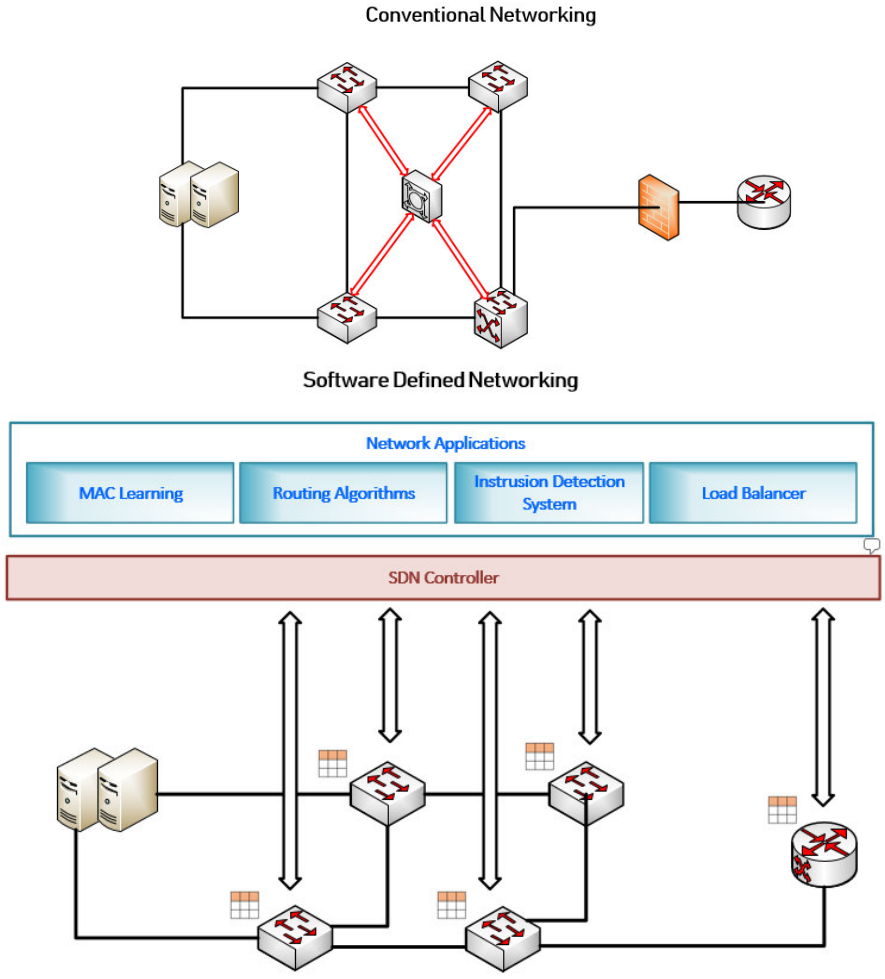


Figura 2.9 Topología convencional de redes y topología basado en SDN [Kreutz Diego – Ramos Fernando M. V. – Esteves Veríssimo Paulo – Esteve Rothenberg Christian - Azodolmolky Siamak - Uhlig Steve, 2014, Redes definidas por software (SDN): una encuesta exhaustiva]

El gran acoplamiento que existe entre los planos de control y datos en la estructura de red tradicional, dificulta la adición de nuevas funcionalidades a las redes de datos, el acoplamiento de los planos de control y datos (y su incorporación física en los elementos de la red) propicia que el desarrollo de la red y la implementación de nuevos algoritmos de enrutamiento sean

complejos, dado que implicaría una modificación del plano de control en todos los dispositivos de red por medio de la instalación de nuevo firmware y, en algunos casos, implicaría actualizaciones de hardware. Por consiguiente, las nuevas funciones de red se presentan comúnmente mediante equipos costosos, especializados y complejos en su configuración como balanceadores de carga, sistemas de detección de intrusos, firewalls. Aquellos dispositivos deberán colocarse en la red, lo que dificulta el cambio de la topología, la configuración y la funcionalidad de la red.

En contraste, las redes definidas por software (SDN) desacoplan el plano de control de los dispositivos de red y se convierten en el NOS (Network Operating Systems) o controlador SDN. Tiene ventajas como la fácil programación de las aplicaciones, la integración de éstas, es decir, el equilibrio de carga y las aplicaciones de los protocolos de enrutamiento se combinan secuencialmente, donde el balanceo de carga tiene prioridad sobre las políticas de enrutamiento [46].

Las redes informáticas o redes definidas por software, se dividen en tres planos de funcionalidad: Los planos de datos, plano de control y plano de aplicación como se observa en la figura 2.10, que corresponde a la arquitectura de red genérica definida por software

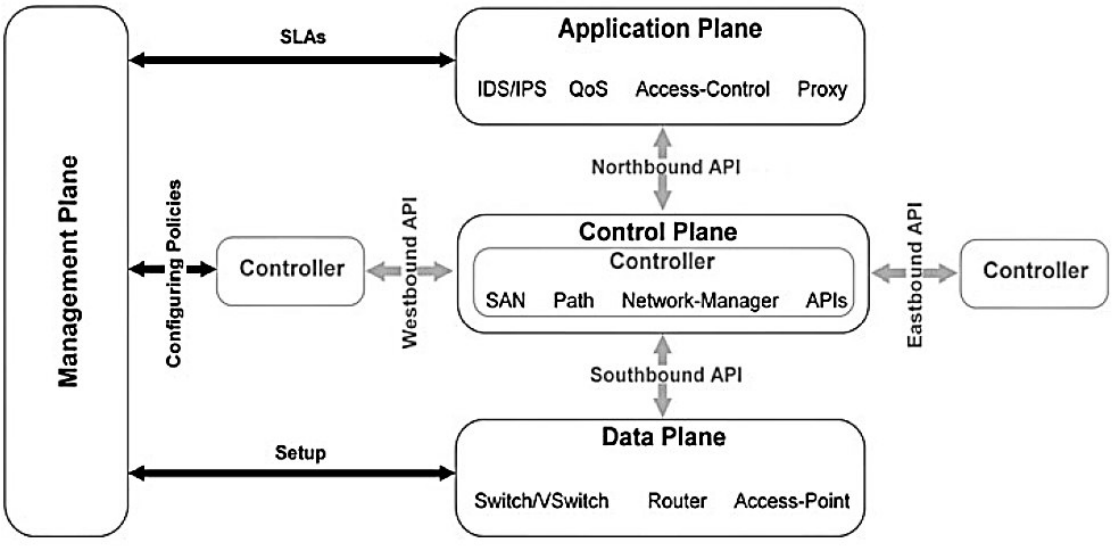


Figura 2.10 Arquitectura de redes definidas por software – SDN [Benzekki Karnal – El Fergougui Abdeslam – Abdelbaki – Elalaoui Elbelrhiti, 2017, Redes definidas por software (SDN): una encuesta]

2.9.1.1 Terminología de las redes definidas por software

1) **Dispositivos de reenvío (FD):** son hardware o dispositivos del plano de datos basados en software que desarrollan un conjunto de operaciones fundamentales. Los dispositivos de reenvío son un conjunto de instrucciones como reglas de flujo que se emplean para realizar acciones en los paquetes entrantes como el caso del reenvío de paquetes a través de puertos, reenvío al controlador, reescribir algunos encabezamientos. Estas instrucciones están definidas por las interfaces southbound (OpenFlow, ForCES) y están instalados en los dispositivos de reenvío por los controladores SDN implementando los protocolos southbound [46].

2) **Plano de datos (DP):** los dispositivos de reenvío están interconectados a través de canales de radio inalámbrico o cableado. La infraestructura de red comprende los dispositivos de reenvío interconectados que representan el plano de datos [46].

3) **Interfaz southbound (SI):** es el conjunto de instrucciones de los dispositivos de reenvío que están definidos por la API southbound, que forman parte de la interfaz southbound. El SI también define el protocolo de comunicación entre dispositivos de reenvío y elementos del plano de control; este protocolo se basa en la interacción de elementos del plano de control y plano de datos [46].

4) **Plano de control (CP):** los dispositivos de reenvío están programados por elementos de plano de control a través de la interfaz southbound (SI). El plano de control por ende se denomina "cerebro de la red". Toda la lógica de control se basa en las aplicaciones y controladores, que forman el plano de control [46].

5) **Interfaz Northbound (NI):** el NOS (Network Operating System) ofrece una API a los desarrolladores de aplicaciones.; esta API representa una interfaz northbound, es decir, una interfaz común para el desarrollo de aplicaciones. Los conjuntos de instrucciones de bajo nivel son aprovechados por las interfaces southbound para programar dispositivos de reenvío [46].

6) **Plano de Gestión (MP):** es el conjunto de aplicaciones aprovechados por las funciones de las interfaces Northbound (NI) para implementar el control de la red y la operación lógica. Comprende aplicaciones como enrutamiento, firewalls, balanceadores de carga, monitoreo, etc. Fundamentalmente, una aplicación de gestión detalla las políticas, que, en última instancia, se descifran a través de las interfaces southbound donde específicamente se programan las instrucciones del comportamiento del reenvío de dispositivos [46].

2.9.2 Gestión y Monitoreo de una Red Definida por Software

El alto interés de la industria y el potencial para cambiar el estado actual de las redes desde múltiples perspectivas, ha propiciado el desarrollo de múltiples esfuerzos para garantizar la estandarización en torno a SDN. Google, ha desplegado SDN para interconectar sus centros de datos en todo el mundo; esta producción en la red ha estado en despliegue durante tres años, ayudando a la empresa a mejorar la eficiencia operativa y reducir significativamente los costos [46].

Una consecuencia importante de los principios de SDN es la separación de las políticas de red, la conmutación existente en la implementación del hardware, y el reenvío de tráfico. Esta separación es fundamental para la flexibilidad, cambiando el problema que existe en el control de los dispositivos de la red, lo que hace que sea más fácil crear e introducir nuevas abstracciones en redes, simplificando la factibilidad, gestión y administración de la red [46].

El plano de datos corresponde a los dispositivos de red, que son responsables del reenvío eficiente de datos. El plano de control representa a los protocolos utilizados para rellenar las tablas de flujo con los elementos del plano de datos. El plano de gestión incluye los servicios de software, un ejemplo de esto es el protocolo simple de administración de red (SNMP), herramienta utilizada para monitorear y configurar de forma remota la funcionalidad del plano de control. La política de red se define en el plano de

gestión; el plano de control hace cumplir la política, y el plano de datos lo ejecuta reenviando los datos en consecuencia [46].

SDN separa las decisiones de enrutamiento y reenvío de los elementos de red (enrutadores, conmutadores y puntos de acceso) del plano de datos y del plano de control para administrar de manera sencilla la red de datos, puesto que el plano de control solo trata la información relacionada con la topología lógica de la red y el enrutamiento de tráfico. En contraste, el plano de datos organiza el tráfico de la red de acuerdo con la configuración establecida en el plano de control. En SDN, las operaciones de control están centralizadas en un controlador que dicta las políticas de la red. Muchas plataformas de controladores son de código abierto como Floodlight, OpenDayLight y Beacon.

La gestión de la red se puede lograr en diferentes capas (es decir, aplicación, control y plano de datos). Los proveedores de servicios pueden asignar recursos a los clientes a través de la capa de aplicación, configurar y modificar políticas de red y entidades lógicas en el plano de control, y configurar elementos físicos de la red en el plano de datos [46].

El control lógicamente centralizado de SDN y las interfaces programables se están utilizando para resolver problemas de fallas de gestión que existen hoy en día. La arquitectura SDN se compone de tres capas: capa de infraestructura o plano de datos, capa de control y capa de aplicaciones [47].

Las capas SDN tienen independencia e interdependencia, vectores de amenaza de tolerancia a fallas, sin embargo existen también vectores de amenaza que necesitan ser tratados. En el plano de aplicación, las fallas se introducen en la red debido a errores de software, afectando la configuración, corrección de red, y fallo de la aplicación de red en conjunto con el plano de control y plano de datos. En la capa de control, afecta a la tolerancia global de fallos en la red; en la capa de infraestructura o plano de datos, la gestión de fallos de enlace o nodo, se relacionan con otros requisitos de red (congestión, calidad de servicio) [47].

CAPÍTULO III

PROPUESTA DE LA TESIS

3.1 NATURALEZA DE LA EMPRESA

Una empresa e-commerce se dedica a la distribución, venta, compra, marketing y suministro de productos o servicios a través de Internet. Originalmente el término e-commerce se aplicaba a la realización de transacciones mediante medios electrónicos, como por ejemplo el intercambio electrónico de datos.

La propuesta de la tesis ha sido desarrollada en una empresa cuya actividad comercial es la venta al por menor de productos diversos. Esta empresa es una Sociedad Anónima Cerrada afiliada a la Cámara de Comercio de Lima, empadronada en el Registro Nacional de Proveedores para hacer contrataciones con el Estado Peruano, nombrada por la SUNAT como Agente de Retención del IGV. La fecha de inicio de actividades de la empresa fue el 24 de enero de 1994.

La empresa administra un conjunto de cadenas de tiendas de diferentes marcas, todas dedicadas al comercio, y es la que brinda servicios de Tecnologías de la Información.

3.2 TOPOLOGÍA DE LA RED DE LA EMPRESA E-COMMERCE

La empresa, al administrar un conjunto de cadenas de tiendas de diferentes marcas, debe tener comunicación de red con todas las sedes remotas que administra (sedes de distribución mayoritaria, tiendas en diferentes centros comerciales y tiendas con puerta a calle).

La empresa cuenta con el servicio housing, contratado al proveedor de internet (ISP) para alojar sus servicios de *web services* en un determinado espacio del centro de datos del ISP.

En la sede central de la empresa existe un pequeño cuarto de comunicaciones o centro de datos, donde se encuentran los principales

equipos de comunicación desde donde se interconectan las demás sedes remotas para hacer uso de los recursos de la empresa como los servidores locales (donde se encuentran almacenados los servicios de *Active Directory*, el endpoint (antivirus) de la empresa y los servidores de dominio de la empresa).

La empresa cuenta con sedes remotas en Lima y provincias, así como en el extranjero, conocidas como franquicias. Cada una de las sedes remotas en Lima tiene el servicio de internet del mismo proveedor que suministra el servicio de internet a la sede central, sin embargo las sedes en provincia tienen contratado diferentes proveedores de internet donde el servicio que se tiene en tienda (sede remota en provincia) es básico y la comunicación a la base de datos es a través de IP pública en lista blanca haciendo uso de una herramienta que proporciona el equipo de seguridad ubicado en el cuarto de comunicaciones o centro de datos de la sede central, cuya solución principal es realizar la interconexión de aquellas sedes remotas a los servidores de la base de datos que se encuentra en la plataforma CLOUD del ISP a través de un software client VPN SSL.

La conexión de las franquicias (sedes remotas en el extranjero) con los servidores de la base de datos en el CLOUD del ISP es a través de VPN IPsec. Esta descripción resume cómo la empresa se intercomunica, a través de la red de datos, con el equipo de seguridad ubicado en el centro de datos de la sede central, para luego realizar consultas a través de una red MPLS a los servidores de producción almacenados en el Cloud del ISP.

La topología de red de la empresa e-commerce analizada donde se desarrollará el prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basado en software libre se detallada en la figura 3.1; donde se presenta el diagrama de la red de datos mostrando los equipos de comunicación que se encuentran en el cuarto de comunicaciones o centro de datos así como los equipos de comunicación distribuidos en los diferentes ambientes de la empresa.

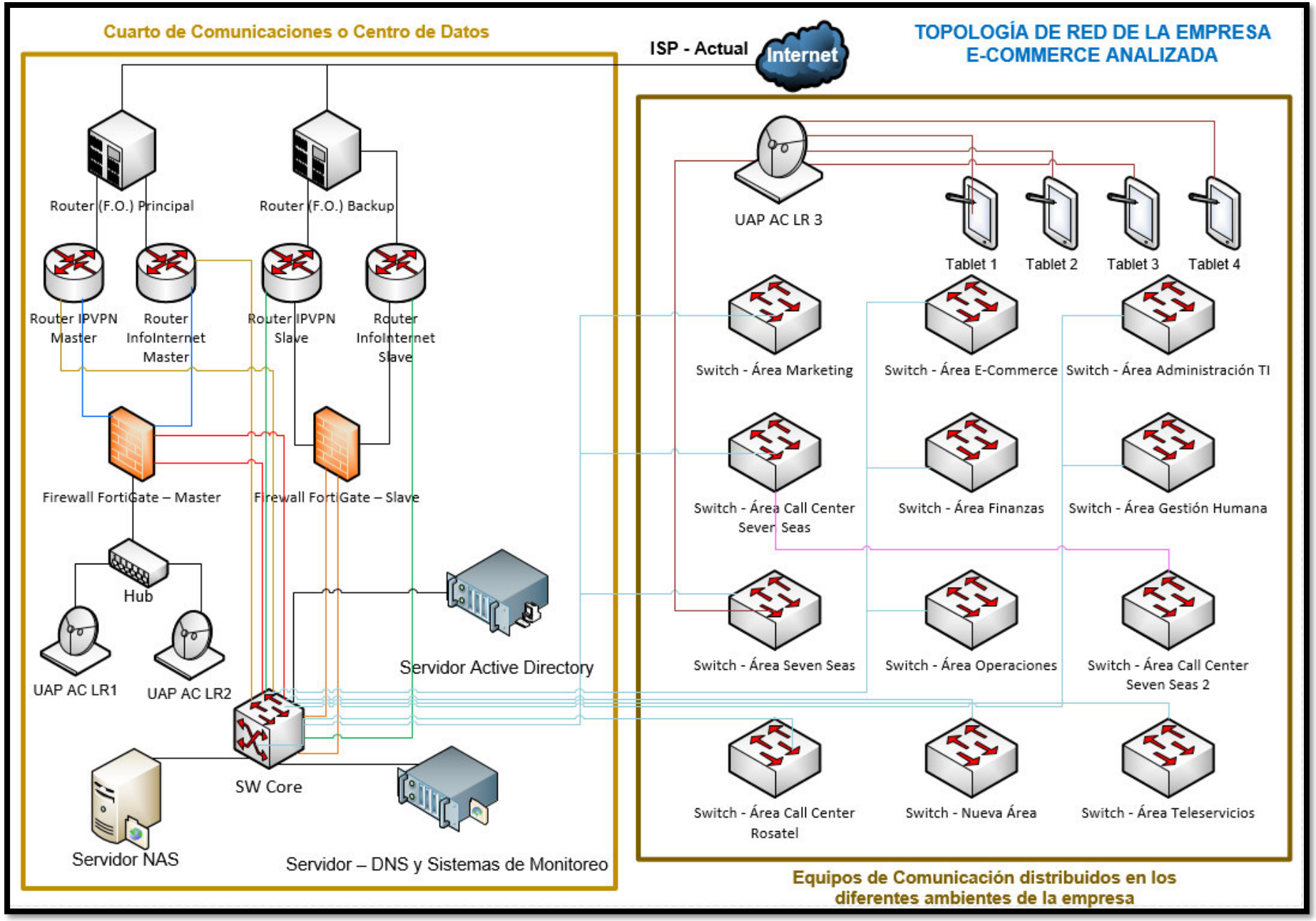


Figura 3.1 Topología de red de la empresa e-commerce analizada [Elaboración propia basado en la información de la empresa]

3.2.1 DESCRIPCIÓN DE LA TOPOLOGÍA DE LA RED DE DATOS DE LA EMPRESA E-COMMERCE ANALIZADA

La empresa en mención tiene 15 sedes a nivel nacional e internacional así como 50 sedes Lima, por lo que requiere un sistema de monitoreo que permita tener el control de los diferentes equipos de comunicación que se encuentran en el centro de datos o cuarto de comunicaciones de la sede central, donde las demás sedes remotas convergen para realizar la interconexión con los servidores de la base de datos, es decir, las tiendas o sedes remotas hacen uso del servicio de IPVPN (conocido como servicio dedicado de datos).

La interconexión se realiza a través de los equipos de comunicación en tiendas, donde existen routers y switches para finalmente interconectar a los equipos finales, donde el router, realiza el enrutamiento hacia el equipo de seguridad de la empresa localizado en la sede central, para finalmente mediante políticas de Firewall direccionar la comunicación de datos a la red MPLS del ISP y con ello mediante enrutamientos realizar interconexión con los equipos de comunicación que forman parte del Cloud del ISP para hacer uso de los recursos de la base de datos que se encuentran en la infraestructura del proveedor de internet (Cloud del ISP).

Recientemente la empresa realizó la migración de ISP, actividad que comprometió la migración completa y compleja de la red de datos y de los *web services* de la empresa. En la sede central se cuenta con equipos de comunicación en alta disponibilidad (HA: High availability) donde el medio de conectividad del ISP a la sede central es a través de fibra óptica, cuyos servicios son de Internet y de datos cada uno en HA conectándose a routers que también se encuentran en HA cuya función principal es recibir el terminal de fibra óptica que llega desde el nodo más cercano del ISP.

Cada router de Tx./Rx. de F.O. es conectado a otros dos routers para brindar servicio de internet y de datos (ambos bajo el escenario de HA), a su vez estos routers que brindan servicios de internet y de datos se conectan a un Firewall que también se encuentra en HA y éste es conectado al Switch Core

donde se conectan los diferentes switches de distribución que administran los puntos de red de las diferentes áreas administrativas y de producción.

Los servidores locales se encuentran conectados en el switch core así como los DVR (Digital Video Recorder o Grabadora de Video Digital) que interconectan las cámaras analógicas permitiendo así la seguridad de la empresa. Los gateways que brindan servicio de Telefonía VoIP para los anexos administrativos y softphones también son conectados al switch core.

En el firewall master o principal y de backup o secundario están conectados dos cables Ethernet hacia un concentrador de red (hub) para interconectar dos APs UNIFI que brindan conectividad WIFI (red WIFI corporativa de la empresa) a toda la sede central.

En los switches de distribución (localizados en los diferentes ambientes de la empresa) se conectan también APs UNIFI para irradiar sectores donde las redes WIFI implementadas en el Firewall Principal y Secundario (implementado de esa manera por el esquema en HA), no alcanzan alumbrar; todo ello es necesario e importante para brindar conectividad vía WIFI a tablets de la empresa que realizan ventas rápidas a través aplicativos o canales alternativos. En estos switches se conectan además los anexos corporativos de la empresa y los equipos biométricos que permiten a través de un sistema instalado en los servidores locales, realizar el control de asistencia del personal administrativo y operativo.

Estos servidores locales almacenan únicamente servicios de seguridad perimetral de la empresa mas no almacenan las diferentes máquinas virtuales que contienen la base de datos de los diferentes aplicativos que administra la empresa y de la cual es propietario. Estos aplicativos se encuentra en la plataforma CLOUD del ISP.

Es importante mencionar la división de los segmentos de red de la empresa para entender un poco más sobre la distribución de los diferentes equipos de comunicación cuya denominación de segmento de red esta nombrada por número de LAN y VLAN.

En la tabla 3.2 se muestra a continuación los segmentos de red subdividas en VLANs que forman parte de las redes privadas de la empresa.

3.2.2 Redes LAN de la empresa e-commerce

Las redes y subredes de la red de área local (LAN) de la empresa, garantizan una adecuada administración y seguridad de la información permitiendo así accesos diferenciados entre las diferentes VLANs que agrupan a un conjunto de usuarios (personal administrativo diferenciado por área), cuyas VLANs fueron inicialmente creados en el equipo de seguridad de la empresa analizada.

Nombre del Segmento de Red	Descripción del Segmento de Red (Subredes)	Red y Subredes	IP/Netmask
LAN1-VLAN2	Admin-Switches	172.20.50.0	172.20.50.1/24
LAN1-VLAN3	Servicio externo	172.20.53.0	172.20.53.1/27
LAN1-VLAN4	Impresoras	172.20.53.32	172.20.53.33/27
LAN1-VLAN5	TI	172.20.51.0	172.20.51.1/24
LAN1-VLAN6	Servidores	172.20.52.0	172.20.52.1/24
LAN2-VLAN7	Call Center	192.168.21.0	192.168.24.254/24
LAN3-VLAN8	Marketing	192.168.35.0	192.168.35.1/26
LAN3-VLAN9	Finanzas	192.168.35.64	192.168.35.65/27
LAN3-VLAN10	Seven	192.168.35.96	192.168.35.97/27
LAN3-VLAN11	RR.HH.	192.168.35.128	192.168.35.129/27
LAN3-VLAN12	Operaciones	192.168.35.160	192.168.35.161/27
LAN3-VLAN13	Servicios en línea	192.168.35.192	192.168.35.193/27
LAN3-VLAN14	Gerencia	192.168.35.224	192.168.35.225/27
LAN4-VLAN15	Teléfonos	10.159.146.0	10.159.146.1/24
LAN4-VLAN16	Video Vigilancia	192.168.13.128	192.168.13.129/25
LAN5-VLAN17	VPNs	172.20.54.0	172.20.54.1/24
LAN5-VLAN18	GPO Administrativo	192.168.36.0	192.168.36.1/24

Tabla 3.2 Descripción de los segmentos de red de la empresa e-commerce [Elaboración propia basado en la información de la empresa]

3.3 PROPUESTA DEL PROTOTIPO DE MONITOREO DE UNA EMPRESA E-COMMERCE

La infraestructura de la sede central de la empresa analizada, aloja un cuarto de comunicaciones o centro de datos, que contiene los principales equipos de comunicación y es donde convergen las 3 sedes remotas, para realizar consultas a la base de datos a través del equipo de seguridad ubicado en el centro de datos de la sede central.

El centro de datos de la empresa contiene importantes equipos de comunicación como el switch Core, los switches de distribución, firewall, APs, servidores, DVR que requieren ser monitoreados para evitar caídas de los diferentes servicios de la cual hacen consumo el personal administrativo de la empresa así como los usuarios y/o clientes de la empresa; por ello surge la necesidad de implementar un prototipo de monitoreo haciendo uso de software libre puesto que son patrocinadas por la Free Software Foundation, bajo la Licencia Pública General de GNU, lo que implica que la empresa ahorre una ostentosa inversión al no tener que invertir en un sistema de monitoreo licenciado.

El presente proyecto de tesis surgió como una propuesta para tener un conocimiento más amplio de los eventos de red y con ello adelantarse a los posibles problemas mejorando los tiempos de respuesta ante incidentes puesto que al ser reportado al ingeniero de redes o administrador de redes de datos, podrá finalmente hacer uso de los recursos necesarios y, a la mayor brevedad posible resolver el problema (que se encontró en el prototipo de monitoreo).

Asimismo, permitirá tomar decisiones adecuadas y oportunas para realizar mantenimiento de los diferentes equipos de comunicación en tiempos efectivos, así como detectar en tiempo real qué dispositivo de comunicación se encuentra causando problemas para analizar detalladamente lo ocurrido y brindar una solución de manera eficiente o finalmente reemplazarlo en su defecto.

Este prototipo de monitoreo permite también predecir con bastante aproximación, a través de registros estadísticos, los futuros acontecimientos midiendo el tiempo de respuesta de los protocolos analizados en los equipos de comunicación.

Este prototipo de monitoreo recolecta información en tiempo real de los dispositivos de comunicación y de los dispositivos que pertenecen a los usuarios finales, permitiendo tomar decisiones idóneas, de acuerdo a los resultados obtenidos y a lo diagnosticado.

La figura 3.3, es un diagrama (topología de red) que describe la interconexión de los diferentes dispositivos de comunicación y dispositivos finales pertenecientes a las diferentes sedes (sede principal y 3 sedes remotas) donde los equipos monitoreados son aquellos que presentan una etiqueta con el nombre SNMP, puesto que es el protocolo utilizado para la gestión y monitoreo de los dispositivos de comunicación y dispositivos finales.

El prototipo de monitoreo recolecta información en tiempo real del estado y funcionamiento de los equipo y/o dispositivos de comunicación así como de los dispositivos que pertenecen a los usuarios finales (personal administrativo de la empresa) a través del protocolo SNMP, información consolidada en un prototipo de un sistema de monitoreo que brinda información a través de reportes sobre el estado de los dispositivos, referido a la conectividad en tiempo real de los dispositivos en la red, además mide el tiempo de respuesta de la entrega y recepción de paquetes que fluyen por los dispositivos de comunicación y finales haciendo uso de los diferentes protocolos anidados en los servicios y aplicaciones de la empresa.

Permite además mostrar notificaciones a través de eventos que describen lo ocurrido así como actualización de éstos cuando el problema encontrado en tiempo real ha sido resuelto y atendido por el equipo de especialistas y técnicos de redes y comunicaciones.

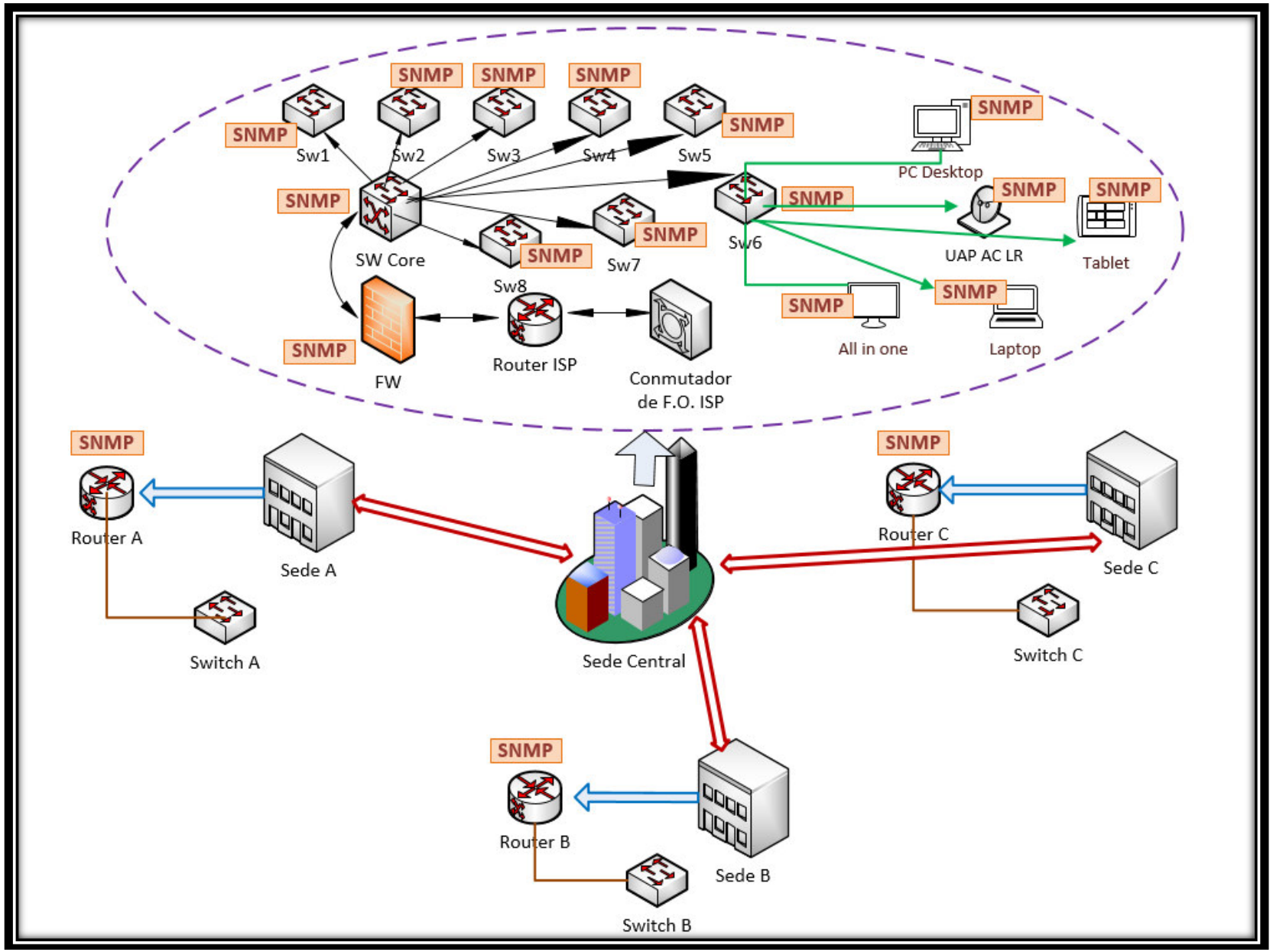
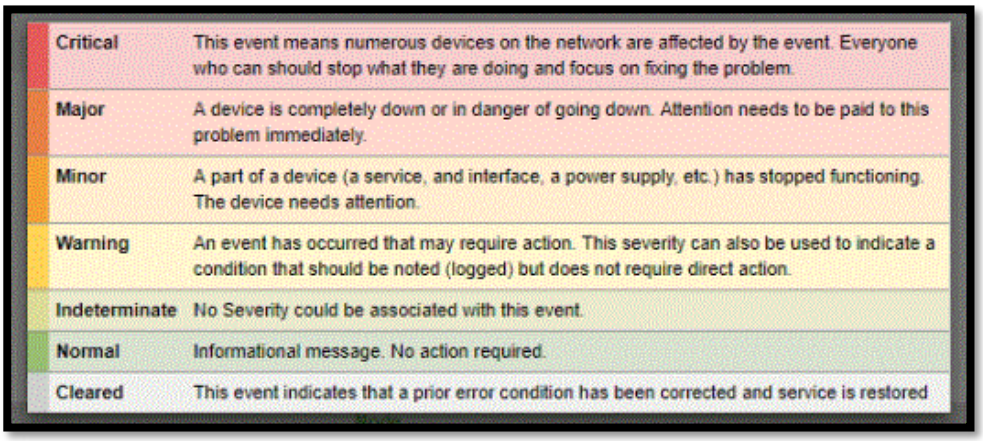


Figura 3.3 Interconexión de dispositivos de comunicación y finales que son monitoreados [Elaboración propia basado en la información de la empresa]

La información que brinda el prototipo de monitoreo es a través de eventos controlados por un proceso que recibe y graba toda la información. Registra todo tipo de eventos: Triggers, automatización de acciones en función del proceso de la tabla de alarmas y evaluación de eventos.

Las alarmas son clasificados en siete secciones representadas por colores diferentes: Color rojo representa una alarma crítica, color naranja representa una alarma mayor, color ambar representa una alarma menor, color amarillo repesenta a una alarma que denota peligro, color verde limón representa una alarma indeterminada (alarma no presentada con frecuencia en el prototipo de monitoreo), color verde representa una alarma que denota un estado normal y finalmente el color plomo que indica que se corrigió una condición de error anterior y se restauró el servicio.

En la figura 3.4 se presenta la clasificación de las alarmas utilizadas en el prototipo de un sistema de monitoreo.



Critical	This event means numerous devices on the network are affected by the event. Everyone who can should stop what they are doing and focus on fixing the problem.
Major	A device is completely down or in danger of going down. Attention needs to be paid to this problem immediately.
Minor	A part of a device (a service, and interface, a power supply, etc.) has stopped functioning. The device needs attention.
Warning	An event has occurred that may require action. This severity can also be used to indicate a condition that should be noted (logged) but does not require direct action.
Indeterminate	No Severity could be associated with this event.
Normal	Informational message. No action required.
Cleared	This event indicates that a prior error condition has been corrected and service is restored

Figura 3.4 Clasificación de alarmas
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

Las notificaciones o eventos obtenidos por el prototipo de monitoreo generalmente son alarmas que denotan eventos mayores, menores y estados de peligro al momento de analizar los dispositivos de comunicación y equipos finales.

Las alarmas son registros de la información que el prototipo de monitoreo recolecta de los nodos, denotación que se brinda a los dispositivos evaluados que utilizan servicios o recursos como aplicaciones propietarias de la empresa. Existen dos procesos en la recolección de eventos, uno llamado

event translator y otro llamado *pasive status* que permiten mapear los eventos de los nodos. El proceso *actiond* permite generar acciones Java basado en eventos que fueron recepcionados. Otro medio para exportar eventos específicos es através de la implementación de XMLRPCD.

En la figura 3.5 se muestra el diagrama de cómo se formula un evento, para reportar al administrador de red incidencias a través de alarmas y/o notificaciones. En el desarrollo del prototipo se utilizó OpenNMS, que se basa en una publicación y suscripción bus de mensajes. Los eventos pueden ser configurados para generar alarmas.

Un evento es generado cuando el Trapd y Syslogd permiten al prototipo de monitoreo recibir capturas SNMP y datagramas de syslog para convertirlos en eventos, luego en alarmas y/o notificaciones.

Trapd maneja el procesamiento de datos de captura SNMP. Los eventos representan un historial de información de red, las alarmas pueden ser utilizados para crear el flujo de trabajo de correlación. Los eventos pueden generar notificaciones vía e-mail, SMS, XMPP y métodos de notificación personalizadas.

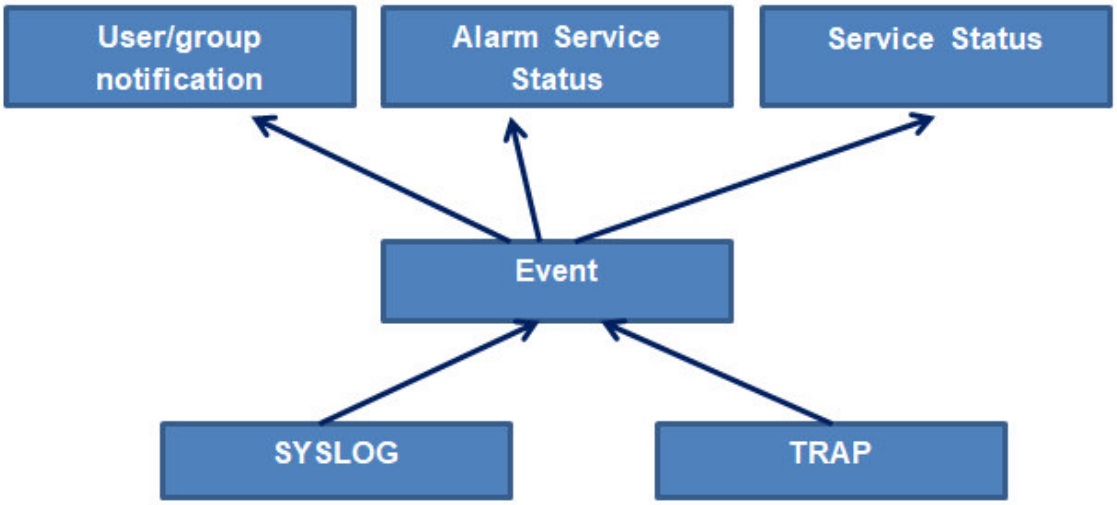


Figura 3.5 Gestión de evento y alarma
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

Los eventos son controlados a través del proceso *Eventd,* proceso que recibe y graba toda la información. Este proceso escucha en el puerto 5817 y por este proceso por el cual se envían peticiones.

Monitorear una red congestionada implica que el protocolo TCP se comporte de manera deficiente con aproximadamente el 5% de pérdida de paquetes y exprese un ineficiente comportamiento al 33% de pérdida de paquetes por lo que el protocolo UDP tendrá éxito eventualmente en este tipo de casos, por ende elegir una medición (testeo) del protocolo UDP a través del puerto 161, que permite capturar datos a través del protocolo SNMP, será la decisión correcta y apropiada para escanear el servicio activo de SNMP en los nodos, definidos anteriormente a los dispositivos terminales evaluados.

En la figura 3.6 se observa la prueba del testeo o scan del servicio activo de SNMP en algunos nodos de equipos terminales ubicados en áreas administrativas.

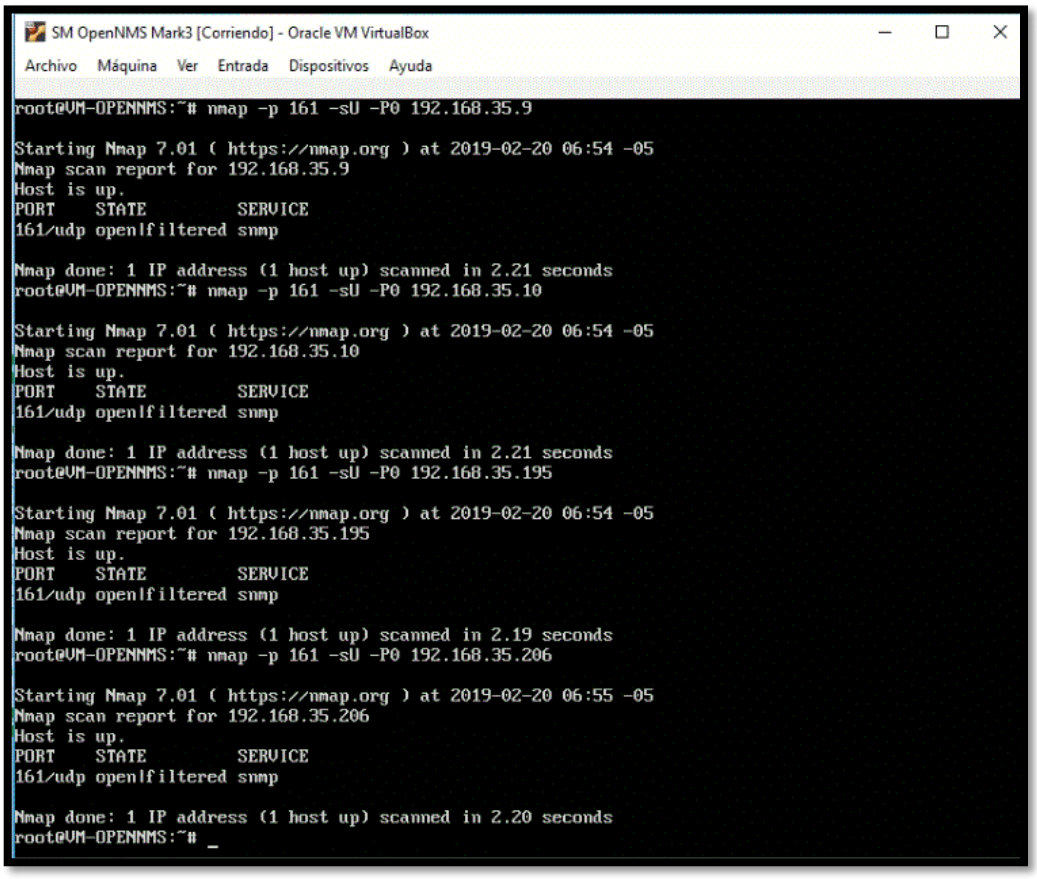


Figura 3.6 Testeo de nodos a través de la herramienta snmpwalk
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

De la figura 3.6 se puede observar que el equipo terminal del ejemplo tiene abierto el puerto 161 UDP, por lo tanto hay un servidor SNMP habilitado en ese puerto. Con el programa de código abierto NMAP que sirve para efectuar un rastreo de puertos así como para descubrir serivicios, permite enviar paquetes definidos a otros equipos y analizar respuestas.

3.3.1 Topología del prototipo de monitoreo propuesto

El prototipo de monitoreo propuesto, fue desarrollado en un host (equipo terminal de la empresa analizada) cuyos parámetros de red pertenecen a la subred LAN3-VLAN14.

Se encuentra implementado en un servidor (máquina virtual), haciendo uso de Oracle VM VirtualBox y del sistema operativo Linux de la versión Ubuntu (64 bits).

En la figura 3.7 se observa la topología de red y la ubicación del prototipo de monitoreo, alojado en un dispositivo terminal, donde el servicio de internet es provisto por un switch de distribución (administrable) que ha permitido realizar el escaneo de toda la red corporativa a través de los dispositivos de comunicación (switch core, firewall, routers).

Este switch de distribución alberga, en una de sus interfaces gigabit ethernet, al dispositivo terminal en el que se encuentra implementado el prototipo de monitoreo propuesto en el presente proyecto.

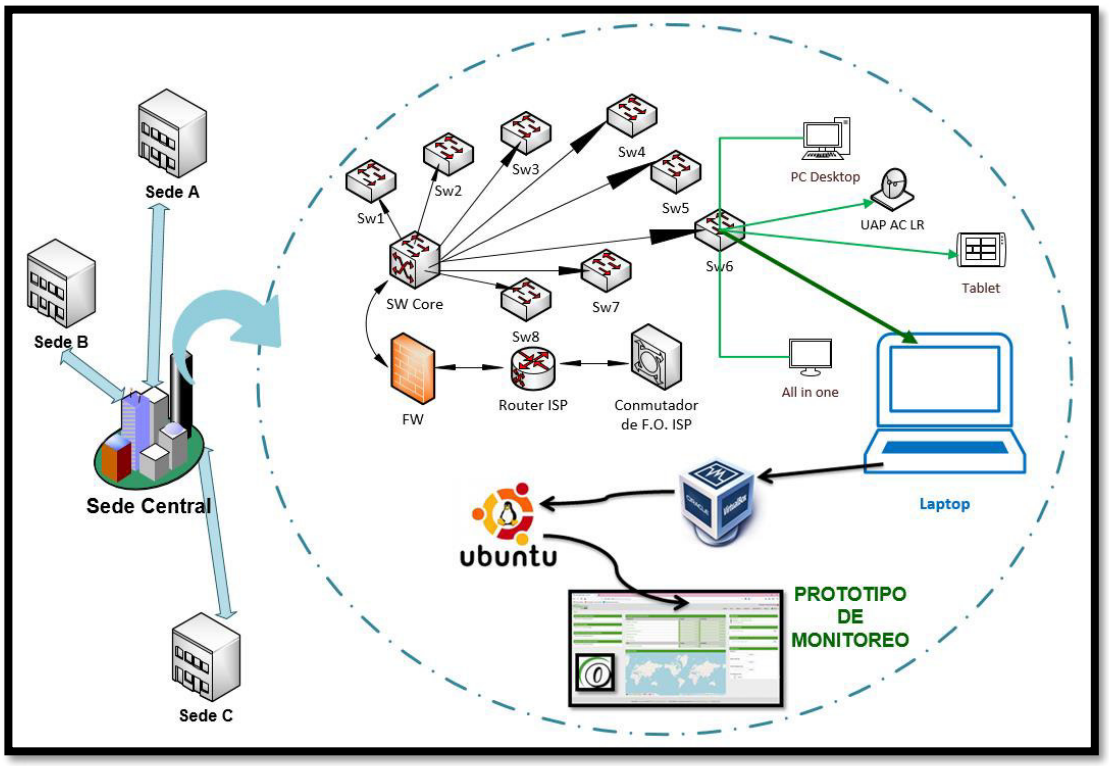


Figura 3.7 Topología de la propuesta de tesis
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

3.3.2 Funcionamiento del prototipo de monitoreo propuesto

El software utilizado para la propuesta de tesis es OpenNMS, cuya arquitectura se presenta en la figura 3.8 a través de un diagrama de bloques en el cual se puede interpretar que el prototipo de monitoreo adquiere información de los dispositivos de comunicación y finales a través de capturas SNMP haciendo uso del proceso TRAPD utilizado para hacer coincidir los traps SNMP (eventconf.xml, archivo de configuración) utilizando una etiqueta (mask), en este proceso las líneas de comandos mib2events y mib2opennms, permiten definir eventos a partir de definiciones MIB.

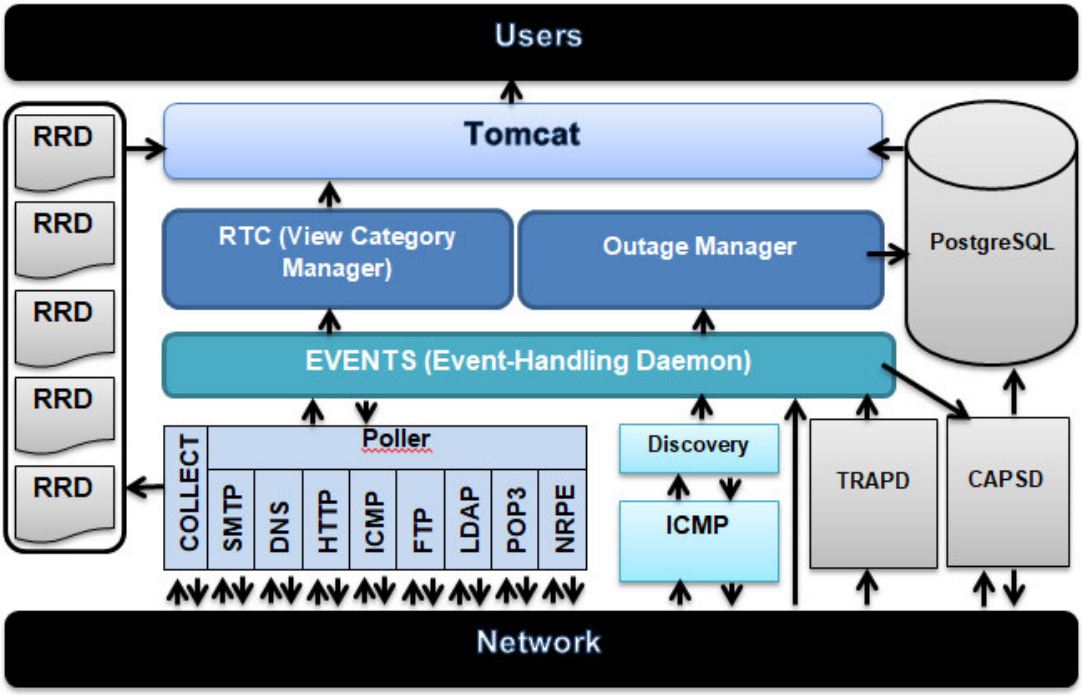


Figura 3.8 Software de la propuesta de tesis
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

CAPSD es un daemon (proceso informático de tipo especial no interactivo, que se ejecuta en segundo plano y no requiere ser controlado directamente por el usuario) que descubre los servicios disponibles y mapea las interfaces SNMP en un dispositivo, este proceso además escucha los eventos (ya sean nuevos o sospechosos) y analiza las direcciones IP en busca de sus capacidades de servicio.

El proceso CAPSD se responsabiliza de descubrir todos los servicios que se monitorean (HTTP, DNS, SMTP, ICMP, FTP, etc.), siendo controlado por el

archivo capsd-configuration.xml. que consta de parámetros básicos como frecuencia de re-escaneo donde CAPSD continuará verificando cada interfaz para ver si se han agregado nuevos servicios y protocolos como 5817 RTC usado para comunicaciones en tiempo real entre el frontend OpenNMS y el motor de backend.

El proceso por el cual se obtiene las capturas SNMP consiste en que el proceso CAPSD intenta recibir el sysObjectID del dispositivo analizado haciendo uso de la comunidad y puerto definido en snmp-config.xml. Al recibir el sysObjectID, el protocolo SNMP se marca como “verdadero” para la dirección IP del dispositivo analizado.

La primera coincidencia válida en el archivo de configuración snmp-config.xml para esa dirección IP, se debe a que dicha dirección IP se incluyó en varios rangos previamente añadidos en el prototipo de monitoreo. Una vez que se analizan todos los protocolos, si el protocolo SNMP es verdadero para la dirección IP, CAPSD realiza pruebas para obtener respuestas de otros servicios monitoreados como SMTP, HTTP, RDP, etc., siguiendo su siguiente secuencia:

- En primera instancia se realizan solicitudes SNMP para recopilar los datos del árbol del prototipo de monitoreo, ipAddrTable (construye un objeto que se utiliza para recopilar los elementos de dirección del agente remoto) e ifTable (agente SNMP normal o un subagente AgentX, cuyo valor predeterminado se ejecuta como un subagente).

- En segunda instancia, las direcciones IP en el ipAddrTable se ejecutan por medio del análisis de capacidades de CAPSD, esto sucede en el escaneo inicial, en los reexámenes y en las reanudaciones normales (de forma predeterminada, cada 24 horas), añadiendo además que las direcciones IP “no administradas” en CAPSD no se sondean.

- En tercera instancia, está comprobado que para cada dirección IP en la ipAddrTable que admite SNMP se le asigna un ifIndex (número de identificación único asociado a una interfaz física o lógica, nombre de la interfaz) válido en el ifTable. Si resulta válido, la dirección IP estará

marcada como interfaz SNMP secundaria y estará apto para cambiar a la interfaz SNMP principal.

- Finalmente, las interfaces SNMP secundarias serán probadas para ver si coinciden con un paquete válido en el archivo de configuración collectd-configuration. Si existe más de una dirección IP válida cumplirán con los tres criterios (compatible con SNMP, posee un índice de if válido y estará incluído en un paquete de recopilación), entonces la dirección IP más baja se marca como principal. Cuando se complete el proceso de prueba de CAPSD, se generarán eventos, incluidos los eventos Node Gained Service.

El descubrimiento (discovery) es la forma en cómo OpenNMS encuentra los nodos (dispositivos con una dirección de red). El descubrimiento puede ser automático o manual, para redes pequeñas como la red analizada en el presente proyecto de tesis, la adición manual de nodos es factible, pero para redes más grandes se beneficiarán significativamente del descubrimiento automático. Antes de iniciar OpenNMS se configuró los rangos de direcciones relevantes (normalmente una o más subredes, donde la sintaxis es flexible). Opcionalmente se configuró cadenas de comunidad SNMP locales, con una flexibilidad significativa en el uso de diferentes cadenas de comunidad para diferentes rangos de direcciones o direcciones específicas.

Una vez configurado, se inició OpenNMS y la red se descubrió automáticamente. El daemon discovery envió pings ICMP para ver si algo respondía en esa dirección IP. Al recibirse una respuesta, se generó un evento "nuevo sospechoso" y se pasó al sistema de eventos OpenNMS. El daemon de capacidades recoge ese evento y escanea esa dirección IP para los servicios disponibles que OpenNMS conoce. El nodo y sus servicios se agregaron a la base de datos OpenNMS comenzando el monitoreo y la recolección de datos para ese nodo. Los eventos que se propiciarán al analizar un nodo son finalmente mostrados al usuario que administra el prototipo de monitoreo a través de alarmas cuya automatización y síntesis de la cantidad de mensajes se debe a syslogd_automations (protocolo de monitoreo).

Para obtener las estadísticas que brinda el prototipo de monitoreo a través de gráficas (archivo de configuración, snmp-graph.properties, incluído en una sección llamada Jboss ejecutada cuando el servicio de JVM ha sido descubierto en el nodo), primero se revisó el archivo collectd-configuration.xml para asegurar de que existe un paquete collectd configurado para recopilar estadísticas JMX (Java Management Extensions, es un agente configurado que se ejecuta en el host remoto para ser monitoreadeo). Dicho archivo cuenta con algunas entradas de Mbean (Objectname es el nombre completo del Mbean "dominio") que hace que el recopilador (JSR 160) recupere las estadísticas de la memoria, en caso esta última acción no suceda, la recopilación de datos se brinda a través de la interfaz JVM (Java Virtual Machine, detector de servicio) del nodo que ofrece el servicio JMX.

Estos resultados internamente son definidos con nombres únicos para Mbeans, donde todos los nombres de objetos JMX tienen dos partes: primero el nombre del dominio JMX, que define el nivel superior dentro del espacio de nombre y un conjunto de parámetros nombre-valor llamado propiedades clave. Es decir si encontramos lo siguiente en el prototipo de monitoreo: (Catalina: tipo= ThreadPool, nombre= http-8080) representa el grupo de subprocesos Mbean para el conector de escucha HTTP en el puerto 8080. En este caso particular el nombre de dominio JMX es "catalina" (nombre del motor de server.xml), tipo es la clase de interfaz de la cual el Mbean es una instancia y "nombre" es el nombre real del recurso administrado.

La propiedad clave que se incluye de forma fiable en los Mbeans (dominios) de Tomcat (Servidor Web que ejecuta Java Servlets) es "tipo". Otras propiedades para el dominio JMX de Tomcat incluyen host, puerto y ruta. La función del motor de la base de datos de PostgreSQL está enfocado en recuperar estadísticas de la base de datos de OpenNMS extendiéndose además a cualquier base de datos de PostgreSQL.

Los sistemas linux tienen un buen gráfico SNMP basados en la estadística de la memoria del sistema. Los procesos generados por el prototipo de monitoreo son registrados por archivos RRD, es decir cuantos más datos se

recopile, se tendrá más archivos RRD, lo cual permite medir el rendimiento de monitoreo, proporcionando suficiente información para anticipar un problema antes de que cause una pérdida de servicio.

El prototipo de monitoreo contiene un sistema de aprovisionamiento avanzado para agregar dispositivos al sistema de gestión. La tecnología subyacente para esta configuración es XML, por lo que se puede utilizar la interfaz de usuario basada en la web o automatizar el proceso mediante la creación de secuencias de comandos de los archivos de configuración XML. El proceso de aprovisionamiento es asíncrona para la escalabilidad; existe la recopilación de datos (de rendimiento) en OpenNMS para una serie de protocolos de red (SNMP, HTTP, JMX, WMI, XMP, XML, NSClient y JDBC), los datos son recolectados, almacenados, graficados y cotejados con umbrales, el proceso es altamente escalable y una instancia de OpenNMS está recogiendo 1,2 millones de puntos de datos a través de SNMP cada cinco minutos.

3.3.3 Parámetros del prototipo de monitoreo propuesto

3.3.3.1 Interfaz web administrativa

Está constituído por 5 componentes:

1. **Vista de vigilancia:** cuando la red es grande y compleja y contienen dispositivos de diferente prioridad, es importante brindar información de lo monitoreado a través de nodos en lugar de servicios, es decir en esta sección se puede observar cuántos de los servidores, switches u otro dispositivo de comunicación tienen problemas, en lugar de cuáles servicios en esa categoría tienen un problema. En la interfaz web administrativa se observa notificaciones de diferentes colores que representan:

   a. Sin caída de servicios: verde - normal
   b. Un servicio inactivo: amarillo - advertencia
   c. Más de un servicio inactivo: rojo – crítico

En la figura 3.9 se observa la vista de vigilancia configurada para monitorear dispositivos de comunicación.

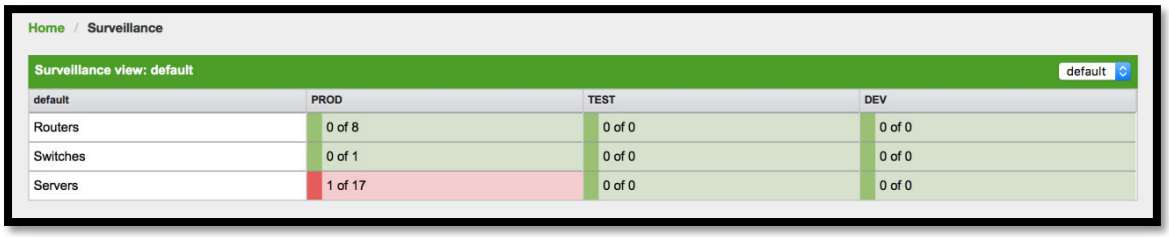


Figura 3.9 Vista de vigilancia de interfaz web administrativa
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

2. **Alarmas:** ofrece una descripción general de todas las alarmas no reconocidas con gravedad superior a la normal, muestra las alarmas más recientes y permite al administrador del prototipo de monitoreo desplazarse por las últimas 100 alarmas. Las alarmas muestran la siguiente información:

   a. Nodo: etiqueta del nodo al que está asociada la alarma
   b. Severidad: severidad de la alarma
   c. UEI: muestra la UEI (identificador único de eventos de OpenNMS) de la alarma
   d. Recuento: número de alarmas duplicadas por la actualización de la misma
   e. Última vez: hora de la última aparición de la alarma
   f. Log Msg: mensaje de registro del evento, fuente de la alarma. Se especifica en el archivo de configuración de eventos en <logmsg />

   En la figura 3.10 se muestra alarmas generadas por el monitoreo de dispositivos de comunicación.

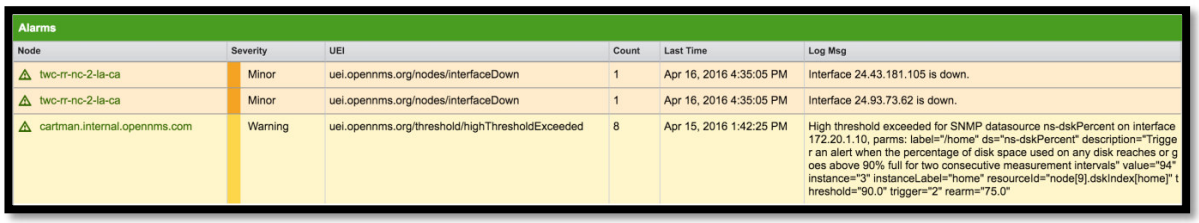


Figura 3.10 Alarmas de interfaz web administrativa
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

3. **Notificaciones:** permite mostrar al administrador del prototipo de monitoreo las acciones que se deben tomar para arreglar o reconfigurar los sistemas de inmediato y resolver un problema en específico

interviniendo en la pronta solución para la continuidad del trabajo del personal administrativo. El campo de las notificaciones muestra las notificaciones no reconocidas que ocurrieron recientemente permitiendo observar las últimas 100 notificaciones. Las notificaciones permiten obtener la siguiente información:

a. Nodo: etiqueta del nodo supervisado
b. Servicio: nombre del servicio al que está asociada la notificación
c. Mensaje : mensaje de la notificación
d. Hora de envío: hora en que se envió la notificación
e. Respondedor : Nombre de usuario que reconoció la notificación
f. Tiempo de respuesta : hora en que el usuario confirmó la notificación

En la figura 3.11 se presenta la información recolectada tras el monitoreo de los dispositivos de comunicación mostrado en el campo notificaciones de la interfaz web administrativa.

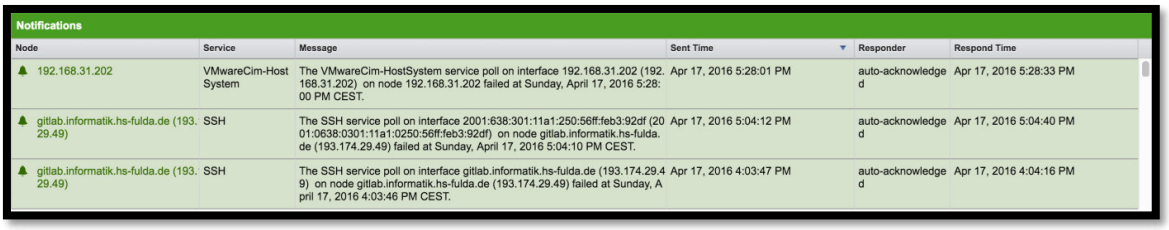


Figura 3.11 Notificaciones en la interfaz web administrativa
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

4. **Estado del nodo:** muestra todas las interrupciones de la red en curso. Al observarse en la interfaz web administrativa una alarma reconocida no significa necesariamente que se solucione la interrupción del servicio. La información mostrada en este campo es la siguiente:

   a. Nodo: etiqueta del nodo monitoreado con interrupciones continuas
   b. Interrupciones actuales: número de servicios en el nodo con interrupciones y número total de servicios supervisados
   c. Disponibilidad las 24 horas: disponibilidad de todos los servicios proporcionados por el nodo calculada por las últimas 24 horas

En la figura 3.12 se proporciona información descrita anteriormente en el campo estado del nodo de la interfaz web administrativa.

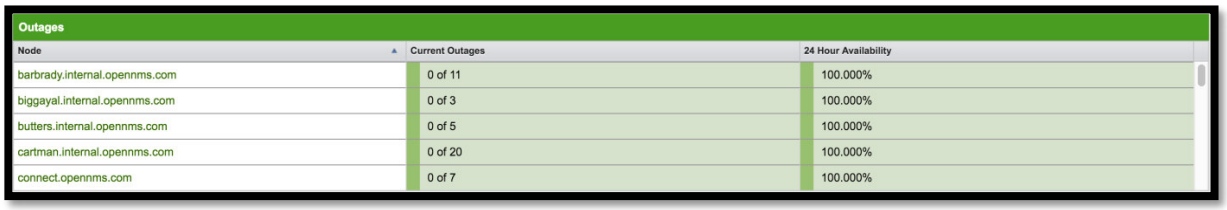


Figura 3.12 Estado del nodo en la interfaz web administrativa
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

5. **Visor de gráficos de recursos:** para brindar un diagnóstico de rendimiento muestra informes de series de tiempo de rendimiento. Este visor gráfico de recursos permite diagnosticar problemas de rendimiento y observar informes de datos de series cuya información es filtrada en el campo vista de vigilancia. Este campo permite navegar secuencialmente a través de los gráficos de recursos proporcionados por los nodos filtrados y seleccionados en el campo vista de vigilancia y muestra un informe gráfico a la vez. En la figura 3.13 se observa la gráfica donde el protocolo monitoreado es DNS (Domain Name Server). La gráfica evalúa el tiempo de respuesta en (ms), es decir mide la velocidad con que se realiza la traducción del nombre de dominio de la empresa en formato dirección IP, y en función de lo rápido o lento que se haga este cambio, así se realizará la carga de las páginas web.

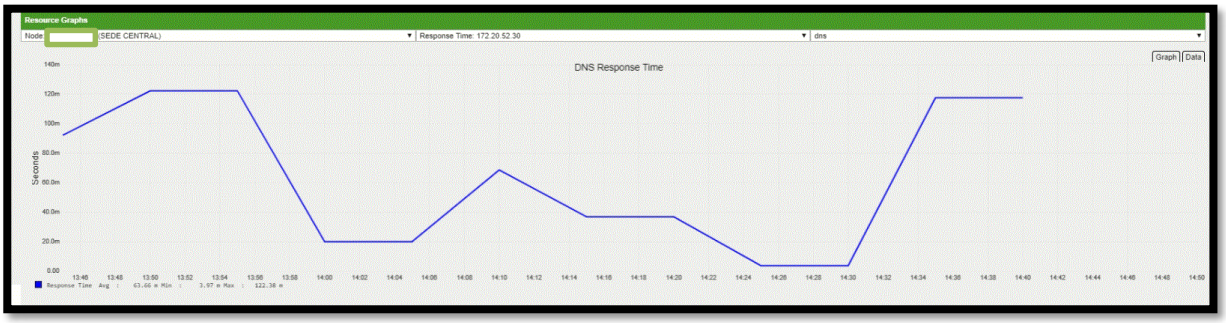


Figura 3.13 Salida de recursos en la interfaz web administrativa
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

Todos estos campos mencionados anteriormente fueron descritos con la finalidad de comprender la visualización general de la interfaz web administrativa que se muestra a continuación en la figura 3.14 donde todos los campos como vista de vigilancia, alarmas, notificaciones, estado del nodo y visor de gráficos de recursos son presentados en una sola pantalla describiendo cada uno de los nodos monitoreados.

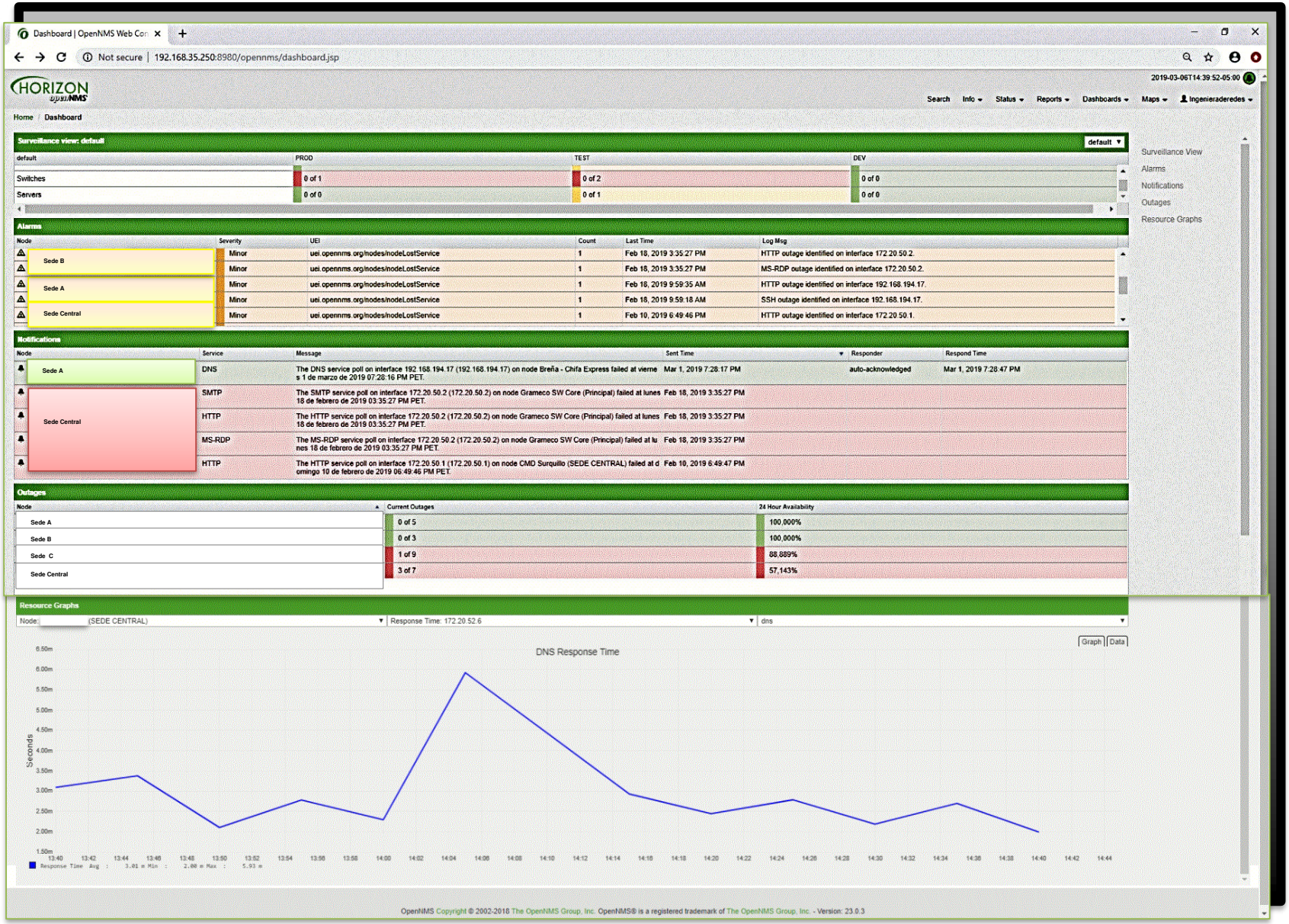


Figura 3.14 Interfaz web administrativa [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

3.4 MONITOREO DE SERVICIOS HACIENDO USO DE PROTOCOLOS UTILIZADOS EN EL PROTOTIPO DE MONITOREO

El prototipo de monitoreo de red propuesto, mide el rendimiento de los dispositivos a través de los protocolos, como ***ICMP*** que administra información relacionada a errores, indicando si un servicio, dispositivo de comunicación o dispositivo final están o no activos.

El protocolo ***TCP/IP*** obtiene información del transporte de datos fiable en un servicio (control de errores, evitar datos duplicados y recuperación ante pérdidas), proporciona control de congestión y evita que la intensidad de tráfico se aproxime a 1 erlang e inicien los encolamientos, e incluso pérdida de paquetes por llenar los buffers de los routers.

El protocolo ***DNS*** indica que el nombre de dominio de la empresa se encuentra operativo, garantizando la comunicación entre los equipos terminales de la empresa evitando pérdida de conectividad a internet en los host de los usuarios administrativos y operativos de la empresa.

El protocolo de transferencia de hipertexto ***HTTP*** determina el estatus de un servidor web y envía periódicamente peticiones para obtener páginas web.

En el caso de un servidor de correo electrónico el prototipo de monitoreo envía mensajes mediante ***SMTP*** (Protocolo de Transferencia de Correo Simple) para luego ser retirados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office).

El protocolo ***RDP*** (Remote Desktop Protocol) muestra el estatus de la comunicación entre la ejecución de una aplicación y un terminal, es decir, indica por ejemplo, si un usuario final puede hacer uso o no de una impresora, que ha sido configurada localmente en un host.

La figura 3.15 es la ventana que se obtiene al hacer clic en un nodo monitoreado de nombre Sede A, ubicado en el mapa urbano que contiene el dashboard. Se observa que el campo “Recent Events” muestra los protocolos monitoreados del router de la sede A.

En este caso en particular los servicios dejaron de estar activos alrededor de las 01:11:07 hrs. hasta las 08:00:00 hrs. aproximadamente, puesto que el personal al retirarse de la sede, desconecta el dispositivo de comunicación de la toma eléctrica y lo enciende al ingresar nuevamente a la sede.

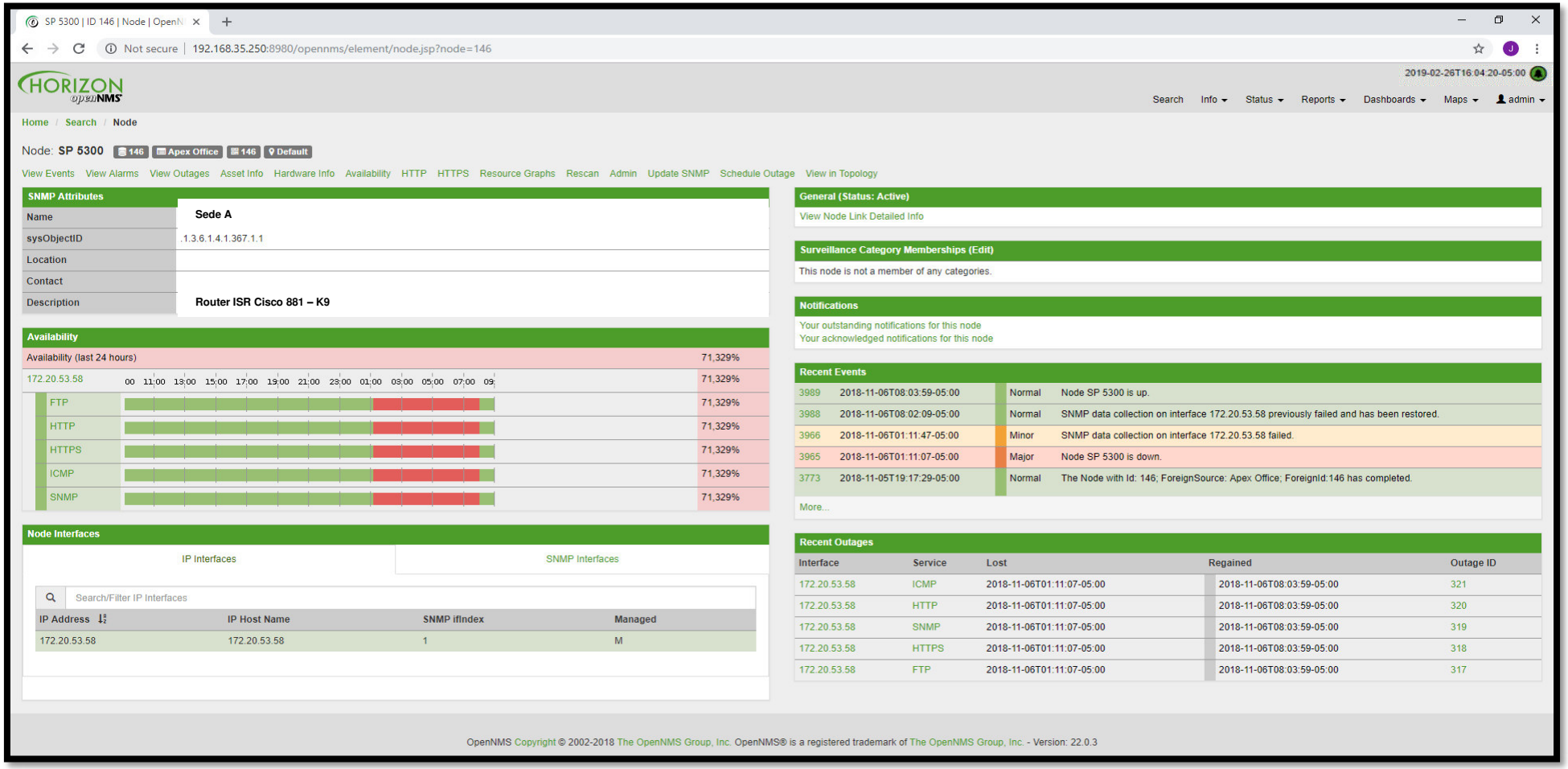


Figura 3.15 Monitoreo del router a través de protocolos de la Sede A [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

CAPÍTULO IV

RESULTADOS

4.1 RESULTADOS OBTENIDOS DEL PROTOTIPO DE MONITOREO

4.1.1 Visión genérica de las funcionalidades del prototipo de monitoreo

El prototipo de monitoreo como se mencionó en el capítulo 3 permite visualizar los nodos, el estado de éstos a través de reportes que se obtienen del monitoreo de protocolos e informados a través de notificaciones, alarmas y eventos que se actualizan cuando el problema ha sido resuelto; permite además obtener información a través de gráficas y brindar un pronóstico de acuerdo a la información recopilada y extraída de la base de datos.

En la figura 4.1 y figura 4.2 se presentan los parámetros medibles del prototipo de monitoreo de red, como nodos que presentan cortes de servicio, alarmas no reconocidas, distribución de severidad, ocurrencias de cortes, ocurrencia de alarmas, cortes de servicio en tiempo real, cuadros estadísticos en relación a tabla de severidad de alarmas, cuadro de interrupciones en los servicios de los nodos monitoreados en los últimos 7 días, interrupciones en tiempo real e inventario de los nodos.

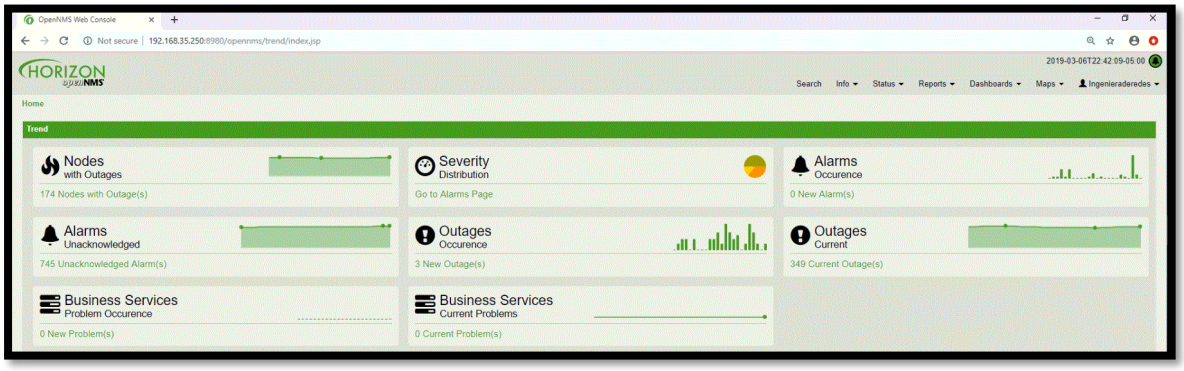


Figura 4.1 Resumen de funcionalidades del prototipo de monitoreo [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

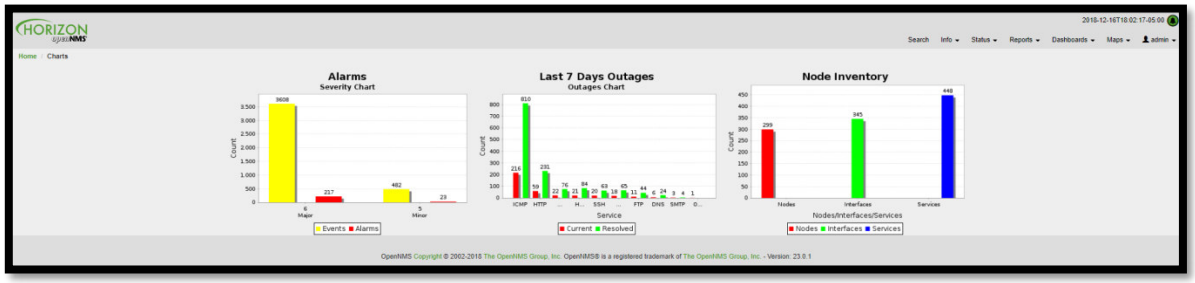


Figura 4.2 Tablas estadísticas – resumen de nodos monitoreados [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

El prototipo de monitoreo de red propuesto, permite evaluar nodos que presentan cortes de servicio así como alarmas propiciadas por el monitoreo de protocolos en el cual el tiempo de respuesta es demasiado alto y existe un problema que resolver en dicho dispositivo de comunicación o terminal monitoreado.

Las tipificaciones de las alarmas que se identifican en el dashboard ubicados en la parte central superior, son presentados a través de anillos que clasifican a los nodos monitoreados en dos secciones: anillo ubicado en el lado izquierdo que contiene nodos monitoreados con alarmas generados por el monitoreo de protocolos y anillo ubicado en el lado derecho que contiene nodos monitoreados con cortes de luz; varían de acuerdo se presente alguna anomalía o incidente y son reportados con un color en específico indicando el estado de los nodos en tiempo real en el panel ubicado en el lado izquierdo.

El dashboard permite además tener un conteo genérico de la cantidad de nodos disponibles.

Finalmente en la parte central e inferior del dashboard se encuentra un mapa urbano donde se encuentran ubicadas las sedes remotas indicando el estado de los nodos monitoreados en dichas sedes.

En la figura 4.3 se presenta el dashboard o interfaz gráfica vía web del software basado en opensource del prototipo de monitoreo de red propuesto en el cual se pueden observar los nodos, categorías y estatus general de los dispositivos monitoreados así como el monitoreo de las sedes A, B y C ubicados en el mapa urbano.

Cada sede remota fue localizada en el mapa con sus respectivas ubicaciones haciendo uso de parámetros como latitud, longitud y zip code. Además, se usó la herramienta de geolocalización HERE WeGo.

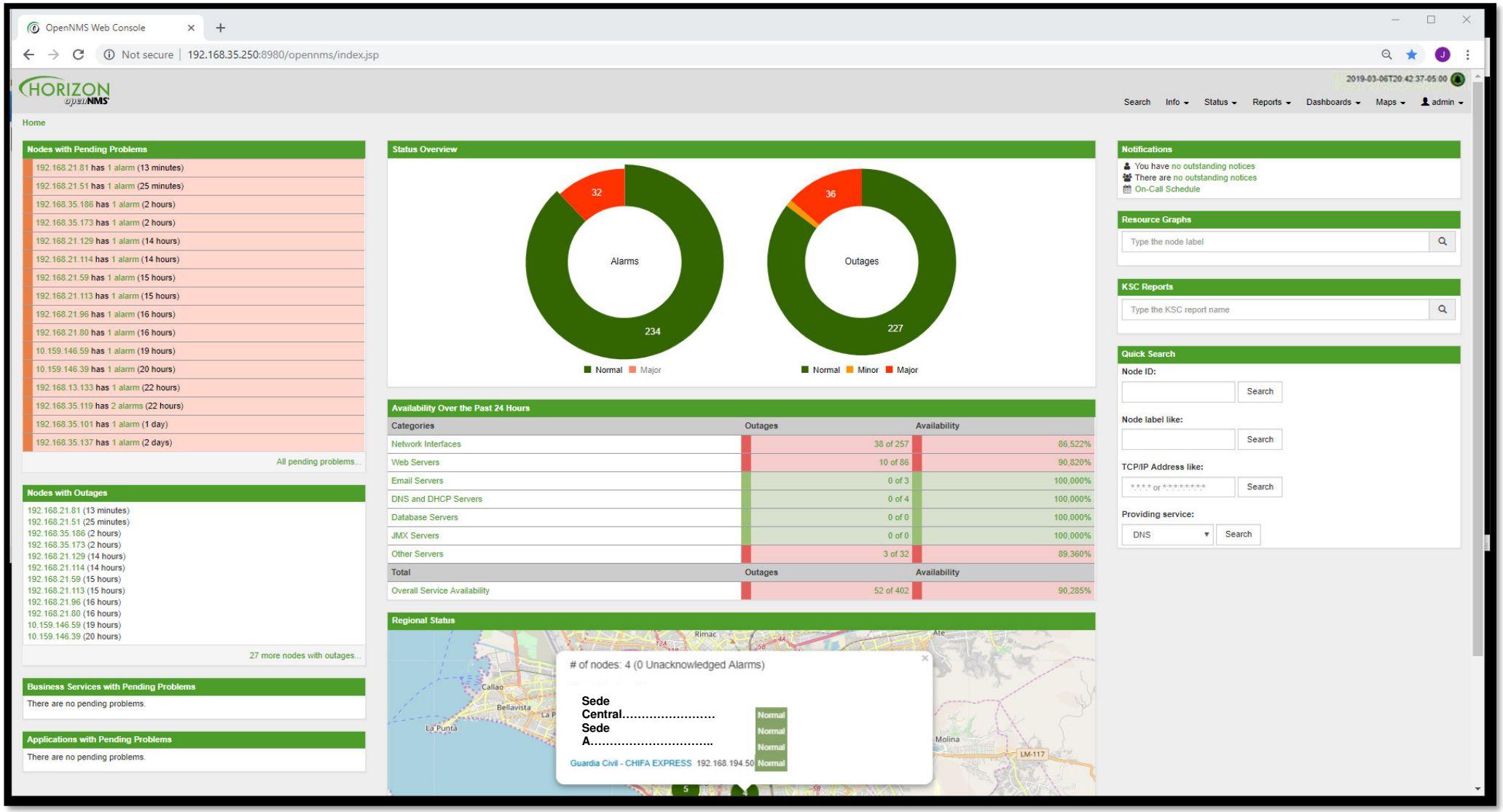


Figura 4.3 Dashboard del prototipo de monitoreo [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

4.1.3 Topología de red de la empresa e-commerce

La topología de red obtenida por el prototipo de monitoreo, muestra los equipos principales (switch core y switches de distribución administrables) que suministran, gestionan y administran los diferentes puntos de red conectados a las interfaces gigabit ethernet de los dispositivos de comunicación los cuales brindan conectividad de red e internet a los dispositivos terminales.

En la figura 4.4 se muestra la topología de red obtenida por el prototipo de monitoreo propuesto en donde se aprecia el gráfico, el listado de los dispositivos de comunicación (switch core y switches de distribución), el tiempo de creación de dicha topología de red, último escaneo de capacidades, interfaz principal, descripción del contacto del dispositivo monitoreado, ubicación del dispositivo y descripción detallada del dispositivo de comunicación o nodo monitoreado.

4.1.4 Alarmas encontradas en la topología de red de la empresa e-commerce

Los diferentes protocolos analizados para cada equipo de comunicación en la red, son mostrados a través de una lista de eventos en el que se detalla los protocolos no operativos en tiempo real.

En la figura 4.5 se presenta debajo de la topología de red de la empresa e-commerce, el listado de las alarmas encontradas para cada uno de los equipos de comunicación, se observan alarmas de color ambar debido a que no todos los sensores responden en conjunto correctamente, lo cual no es realmente alarmente en este caso, puesto que no habrá un corte de servicio, ya que el sensor que no responde es el protocolo HTTP (en uno de los casos) por ejemplo, e indica que no se realizó consulta del switch vía interfaz gráfica en un determinado momento del día. El uso de la interfaz gráfica de un switch en muchos de los casos se utiliza para realizar consulta de los logs y en su defecto para realizar alguna modificación, lo cual no es una actividad recurrente para un administrador de red.

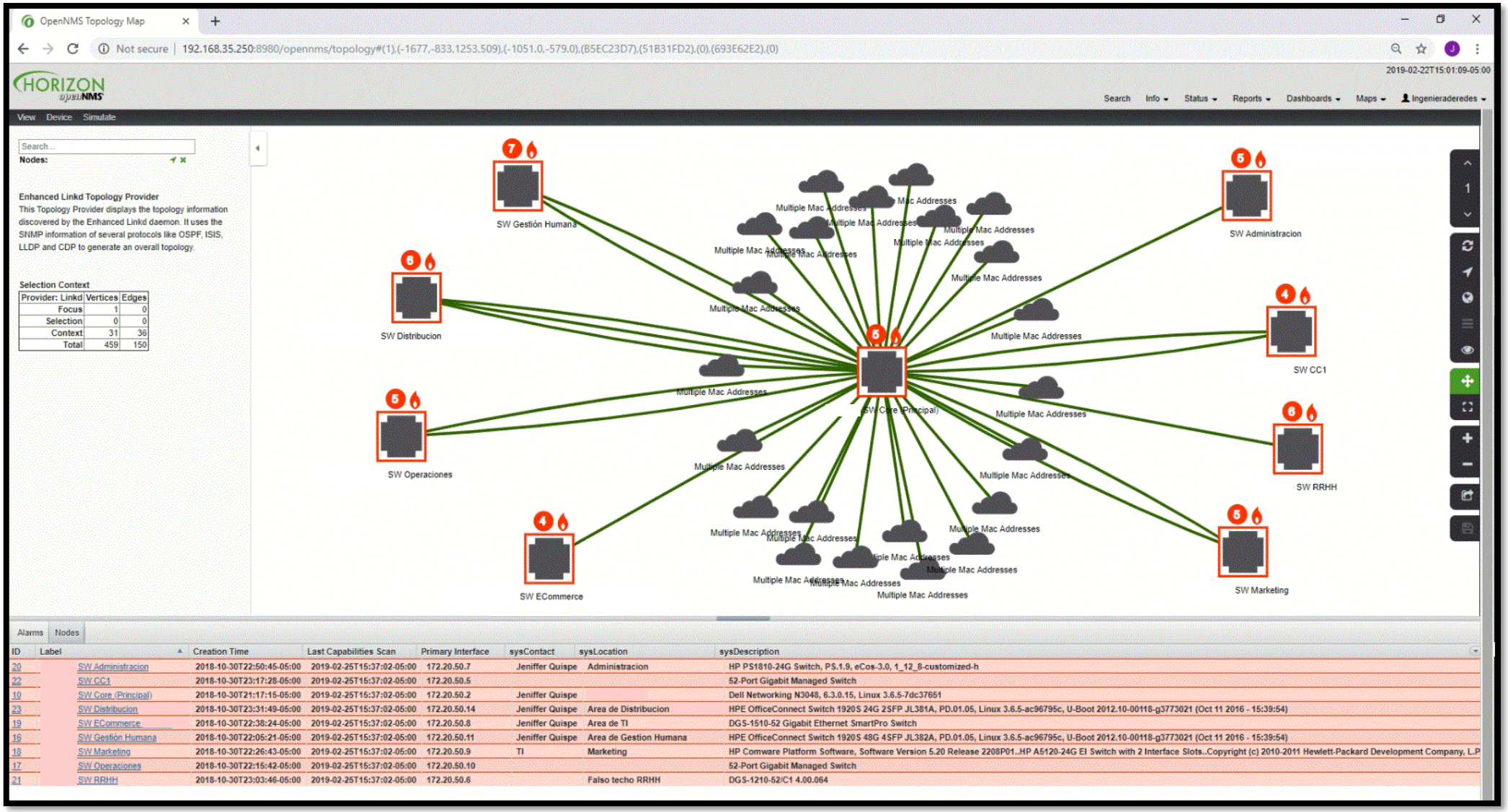


*Figura 4.4 T*opología de red de la Sede Central de la empresa e-commerce analizada [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

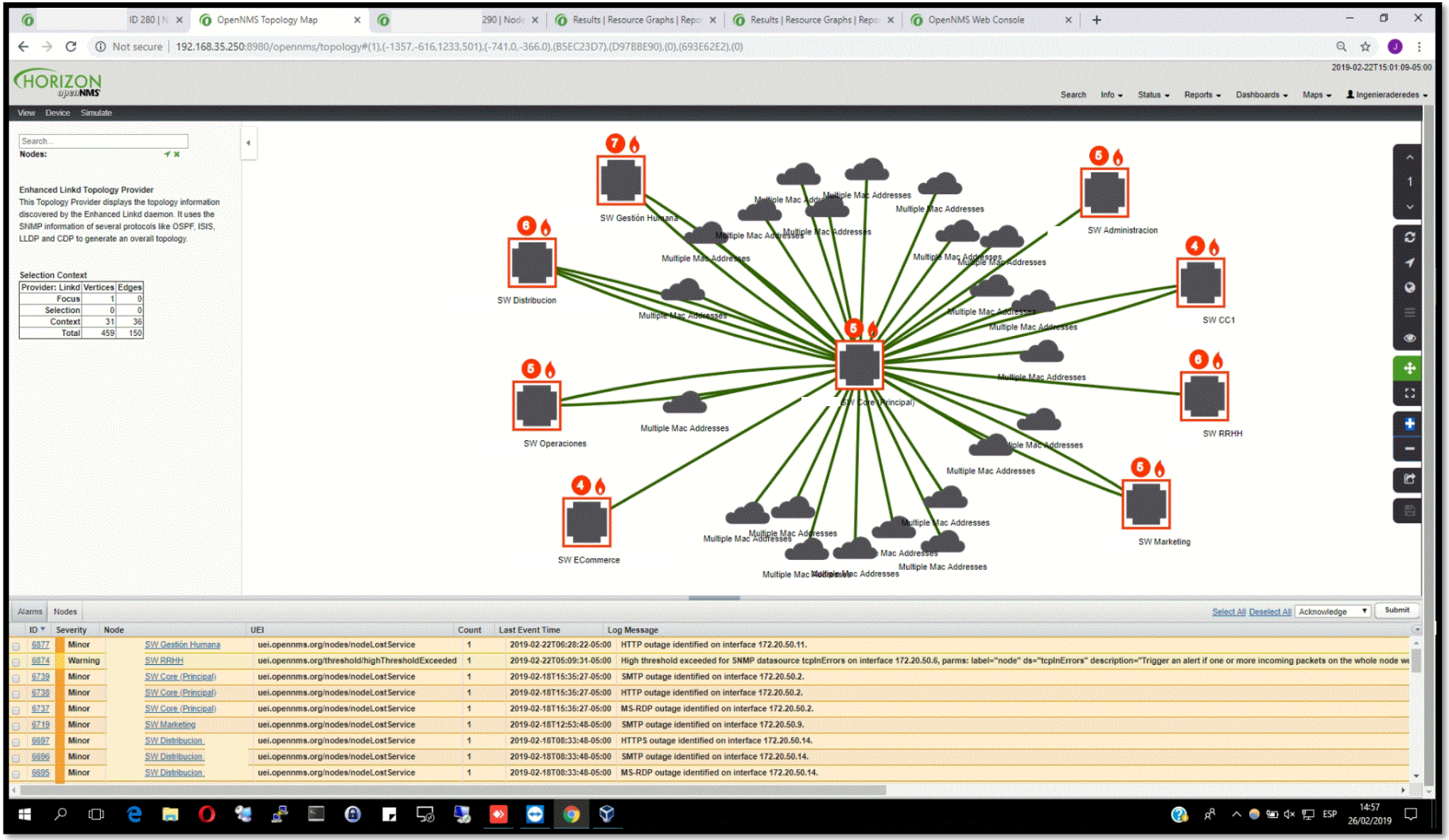


Figura 4.5 Alarmas de nodos en la topología de red de Sede Central de la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

4.1.5 Monitoreo de equipos de comunicación

A. Dispositivos monitoreados de la Sede Central

En la figura 4.6 se muestra el monitoreo de tres equipos de comunicación de gran importancia: equipo de seguridad principal (firewall), DNS Primario y DNS Secundario (servidores locales).

El equipo de seguridad es monitoreado por los protocolos HTTP e ICMP y muestra que hubo corte de servicios por un lapso de cuatro minutos, luego se restablecieron tras haber sido atendido por el administrador de red.

Los DNS primario y secundario alojados en servidores, son monitoreados por los protocolos DNS, ICMP y MS-RDP; hubo un corte en los servicios por un lapso de 10 minutos, restableciéndose, luego de la intervención inmediata del administrador de red al revisar y corregir el problema encontrado. En ambos casos, los problemas se debieron a inconsistencias en el acceso remoto.

La IP privada 172.20.50.1 corresponde al Firewall, la IP privada 172.20.52.6 pertenece al DNS Primario y la IP privada 172.20.52.30 pertenece al DNS Secundario. En la figura 4.6 se muestran los eventos ocurridos para cada equipo de comunicación, tipificados de acuerdo a la clasificación de las alarmas y a los colores que corresponden a cada una de ellas. Cada evento tiene una descripción propia de lo acontecido, mostrando la hora en la que aconteció el incidente, así como la recuperación del incidente, nombrado en el siguiente evento de recuperación del corte del servicio.

En la figura 4.7 se observa el monitoreo de uno de los dispositivos de comunicación (switch de distribución administrable de la sede central). Este switch reparte servicio de conectividad a internet a todo un grupo de personal administrativo que realiza ventas online. Se aprecia que existió un recorte de servicio por 4 horas, y gracias a este prototipo de monitoreo se pudo identificar de inmediato el problema, brindándose troubleshooting a la mayor brevedad posible en conjunto con el ISP, ya que no sólo hubo problemas a nivel físico con el equipo, sino que además hubo una caída del servidor que contiene la base de datos contenidos en el CLUSTER del ISP.

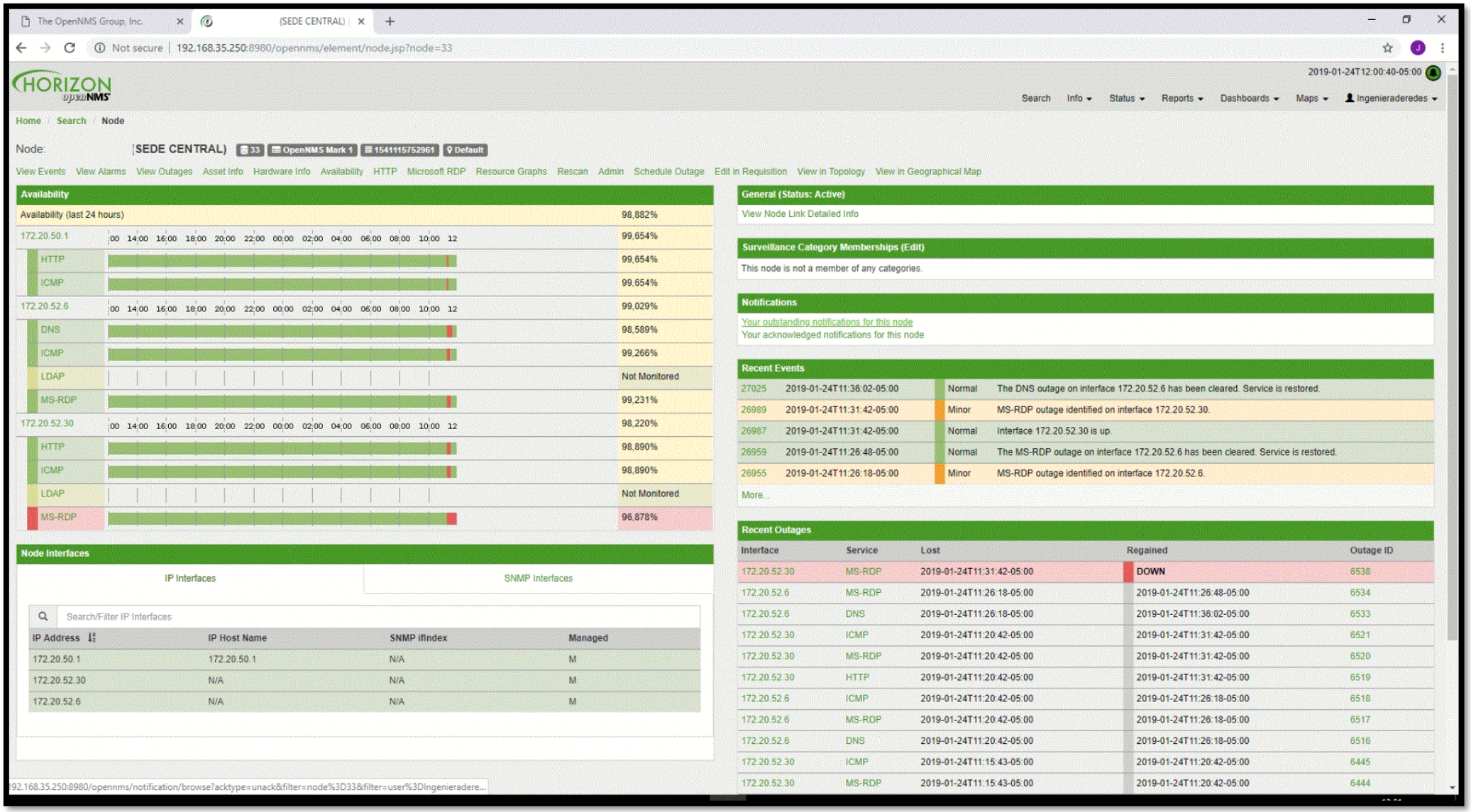


Figura 4.6 Monitoreo de dispositivos de comunicación principal de la Sede Central de la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

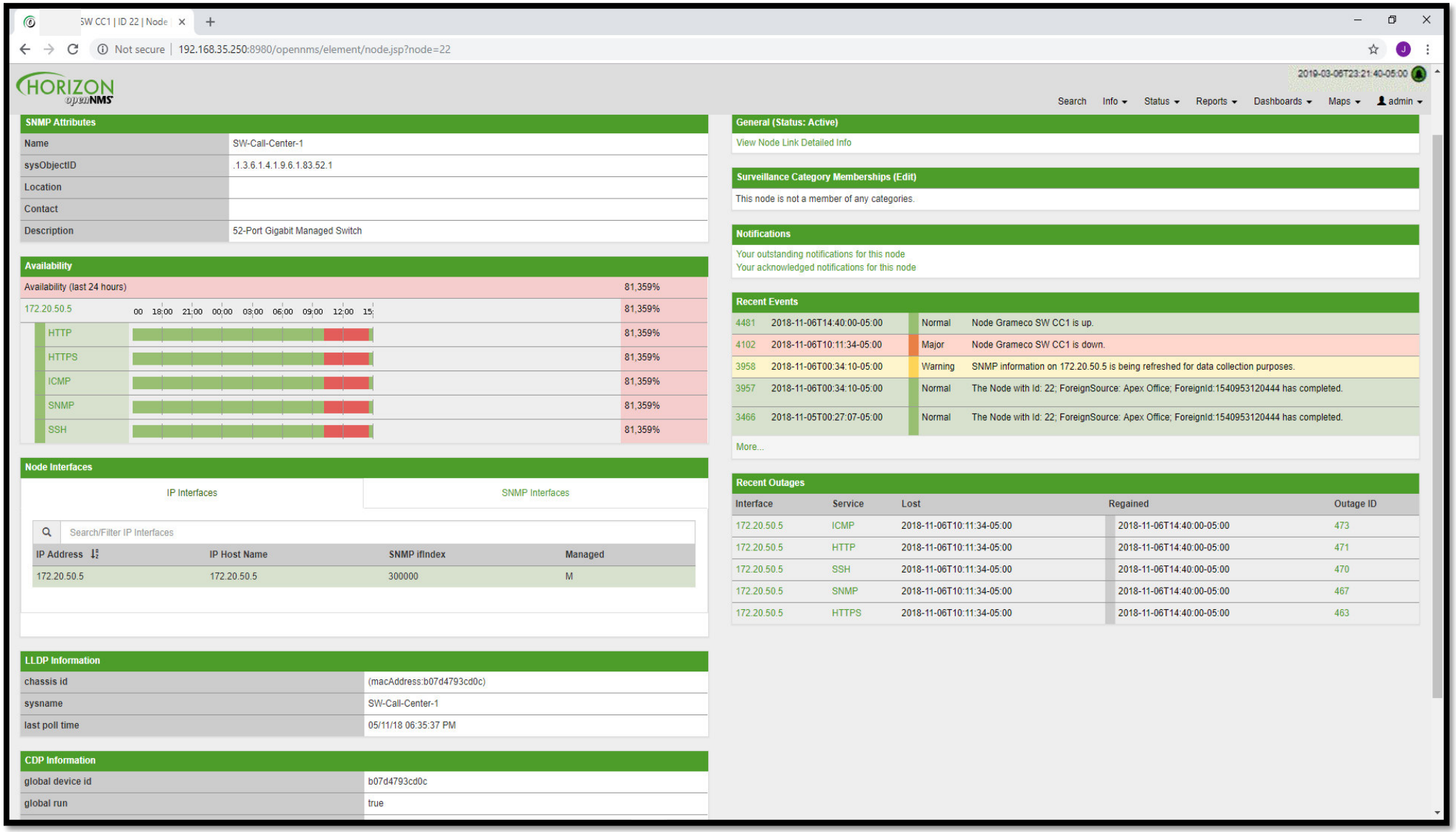


Figura 4.7 Monitoreo de un switch de distribución [Elaboración propia basado en el prototipo de monitoreo de red propuesto]

En la figura 4.8 se muestra el monitoreo de un switch de distribución ubicado en el área de TI; el equipo no presenta anomalías ni incidencias, su operatividad es correcta. Además, se muestran las interfaces gigabit ethernet del switch en funcionamiento y de color verde, que simbolizan que se encuentran operativas y en uso, donde el equipo terminal conectado a esa interfaz puede ser un host, una impresora o un teléfono. Cada equipo terminal también es monitoreado por el prototipo de monitoreo. Finalmente, las interfaces gigabit ethernet de color rojo indican que no se encuentran en uso puesto que no existe velocidad de transmisión de datos. También se aprecia que se usó la herramienta nmap para escanear el puerto 161 UDP, comprobándose que el switch de distribución está siendo correctamente monitoreado en tiempo real.

Asimismo el prototipo de monitoreo permite identificar la marca y el modelo del equipo terminal indicándolo en el campo description.

En la figura 4.9 se observa el monitoreo de un equipo terminal utilizado en su mayoría por el personal administrativo. Este dispositivo terminal es una impresora multifuncional ubicado en una de las oficinas administrativas de la empresa e-commerce analizada, impresora instalada a través de cable de red que puede ser captura en diferentes host a través de la IP privada asignada a dicho dispositivo.

Este dispositivo es monitoreado a través de los protocolos HTTP, HTTPS, ICMP y SNMP. En la figura 4.9 también se puede observar que el protocolo HTTPS dejó de tener servicio desde las 03:57:34 hrs. lo cual en este caso no es un factor determinante puesto que este protocolo permite tener el acceso del dispositivo monitoreado, vía interfaz gráfica a través de la web y puede ser atendido en el transcurso del día ya que no es un problema crítico que comprometa con la funcionalidad y operatividad del dispositivo terminal. Asimismo se hace uso de la herramienta nmap para escanear el puerto 161 UDP, con ello confirmar si el servicio del protocolo SNMP se encuentra activo y asegurar que se realice un correcto monitoreo del dispositivo para recibir información en tiempo real y detectar las incidencias a tiempo, evitando perjudicar el trabajo del personal administrativo.

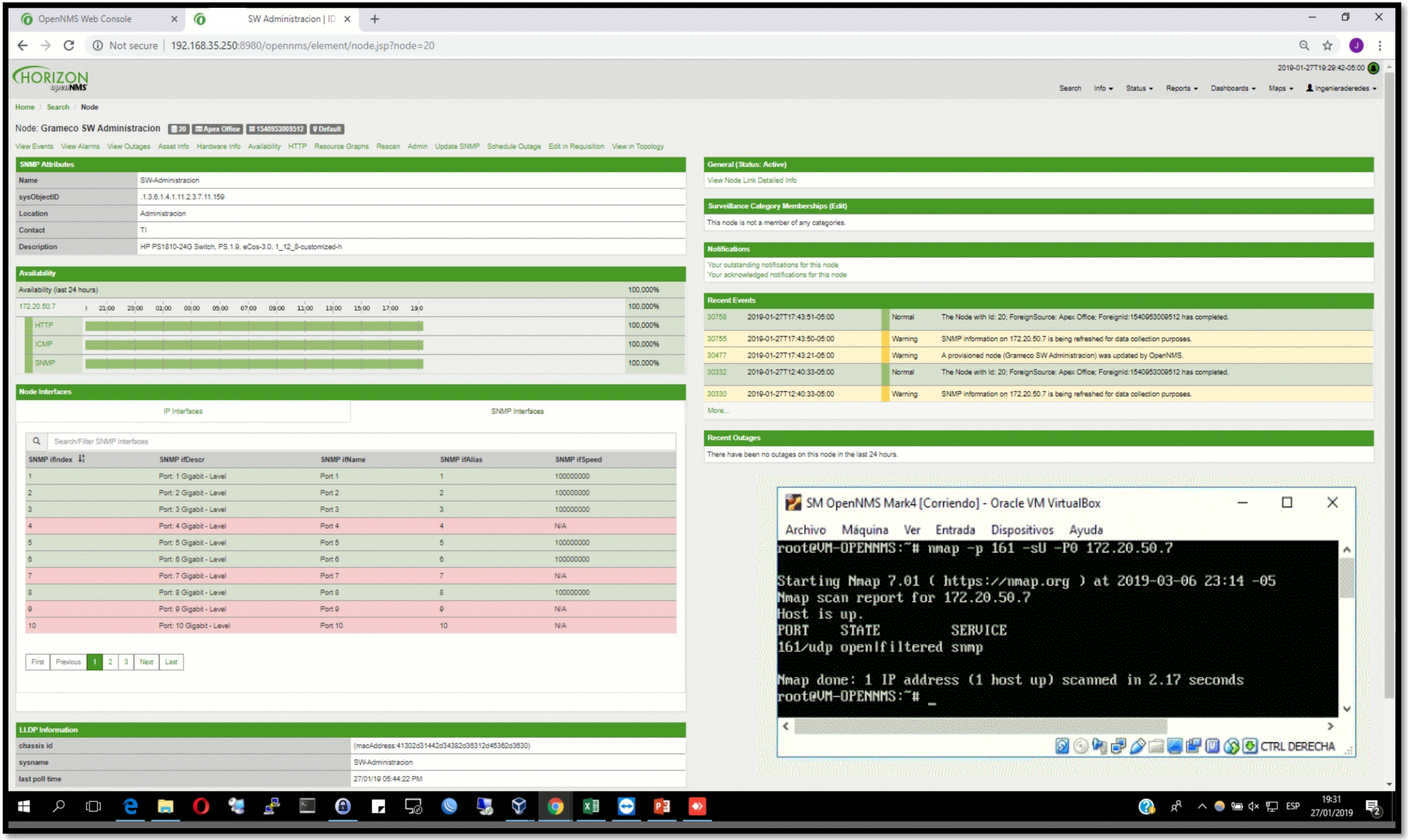


Figura 4.8 Monitoreo de un switch de distribución de la sede central de la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

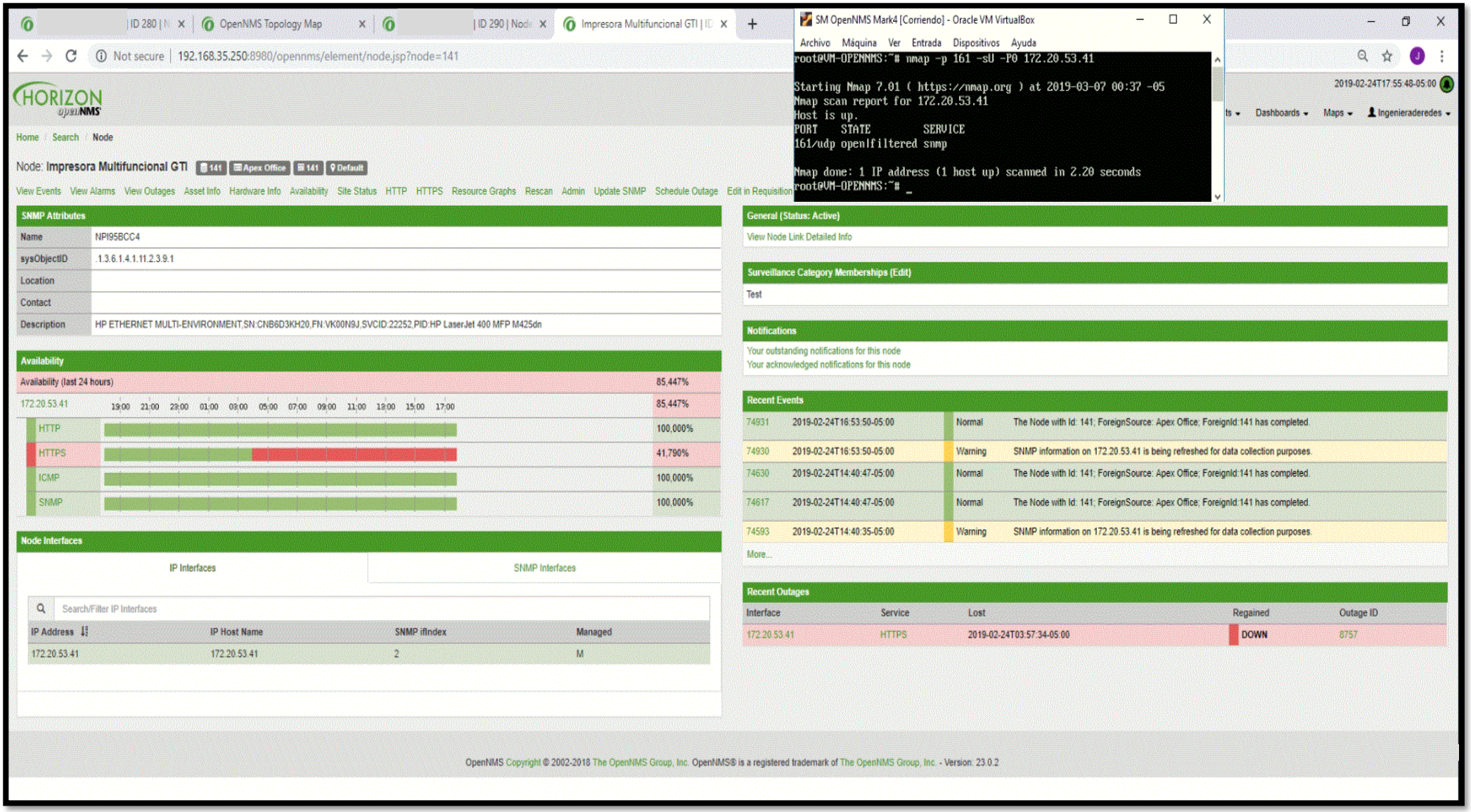


Figura 4.9 Monitoreo de una impresora multifuncional de la sede central de la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

Otros de los dispositivos terminales monitoreados es un teléfono físico, es decir un anexo corporativo, destinado para personal administrativo y personal de ventas que pertenece al área de *call center*. Por ello es de suma importancia conocer el estado de estos dispositivos ya que permiten la continuidad del core del negocio de la empresa. Este dispositivo terminal tiene la IP privada 10.159.146.240 y corresponde al segmento de red LAN4-VLAN15 cuyo nombre de VLAN es Teléfonos- AVAYA.

El monitoreo de este dispositivo terminal se presenta en la figura 4.10 y de acuerdo a lo mostrado en la figura, dicho dispositivo tiene un correcto funcionamiento.

En la figura 4.11 se monitorea un equipo terminal, ubicado en el área de cocina de una de las empresas administradas por la empresa e-commerce analizada. La figura presenta el monitoreo de una laptop ubicada en el ambiente de cocina utilizado por la administradora del área. En la ventana o interfaz gráfica que muestra el monitoreo del dispositivo terminal (laptop), indica que hubo desconexión del equipo a las 23:20 hrs. del día 21.01.2019 puesto que ese día la administradora del área se llevó la laptop a su hogar y retornó a laborar al día siguiente realizando la conexión de la laptop al punto de red en su oficina a las 14:54 hrs. del día 22.01.2019. El día 24.01.2019 la laptop tuvo una falla física por lo que tuvo que ser reparado, por ello existe un evento de caída del nodo a partir de las 11:04 hrs. hasta las 11:41 hrs., tiempo que ha servido al personal de soporte técnico, diagnosticar y solucionar el problema encontrado en el equipo terminal.

La figura 4.12 corresponde a la captura del monitoreo de un equipo terminal desktop con un sistema operativo diferente al común utilizado por la empresa. El protocolo ICMP, sensor que forma parte de la lista de protocolos que monitorea el equipo terminal (PC desktop), no está siendo monitoreado porque el firewall del sistema operativo está activo y está bloqueando el protocolo ICMP, el evento encontrado es el 10.02.2019 y ha servido para realizar una inspección en el equipo terminal y encontrar lo narrado anteriormente.

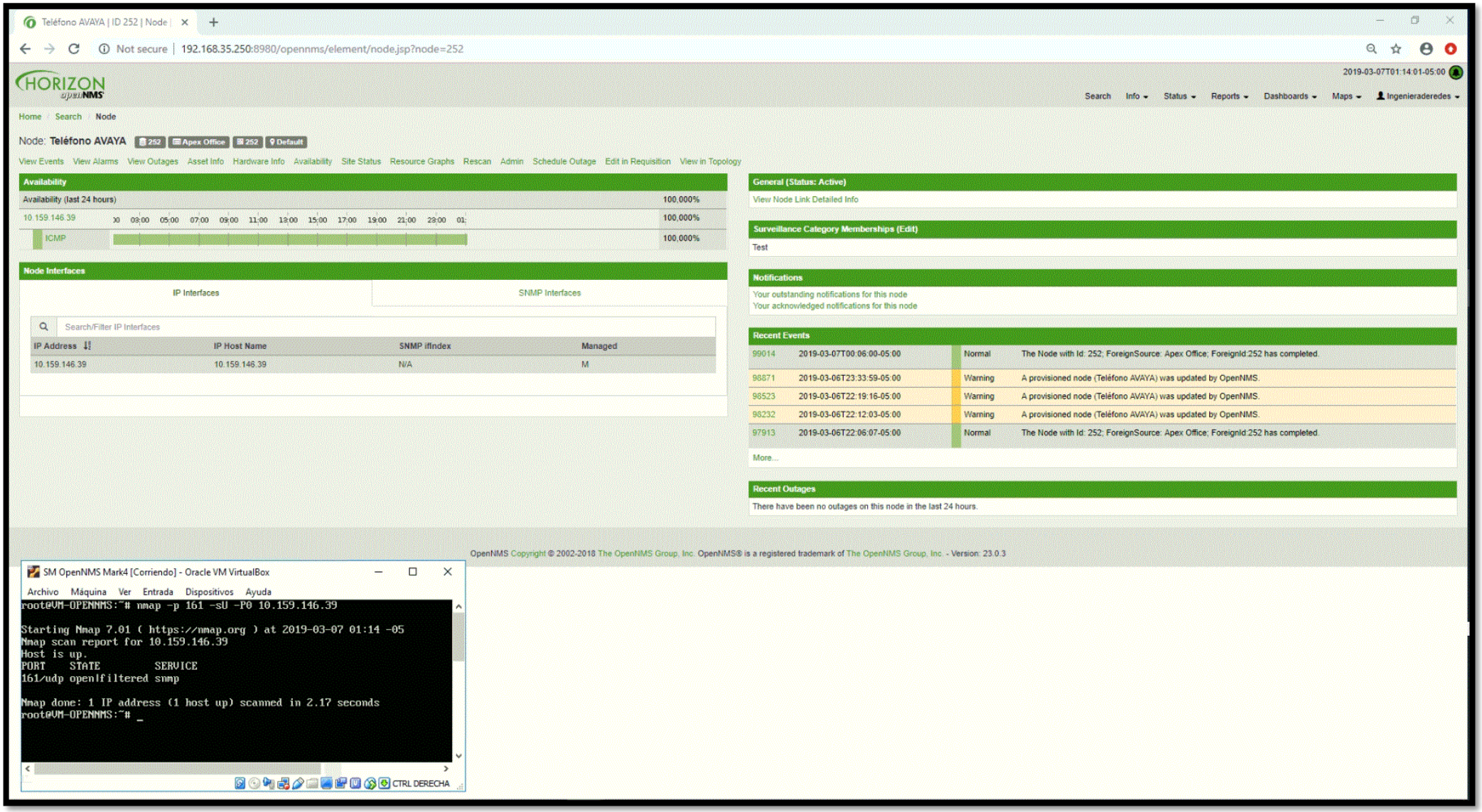


Figura 4.10 Monitoreo de un teléfono físico, anexo corporativo de la sede central de la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

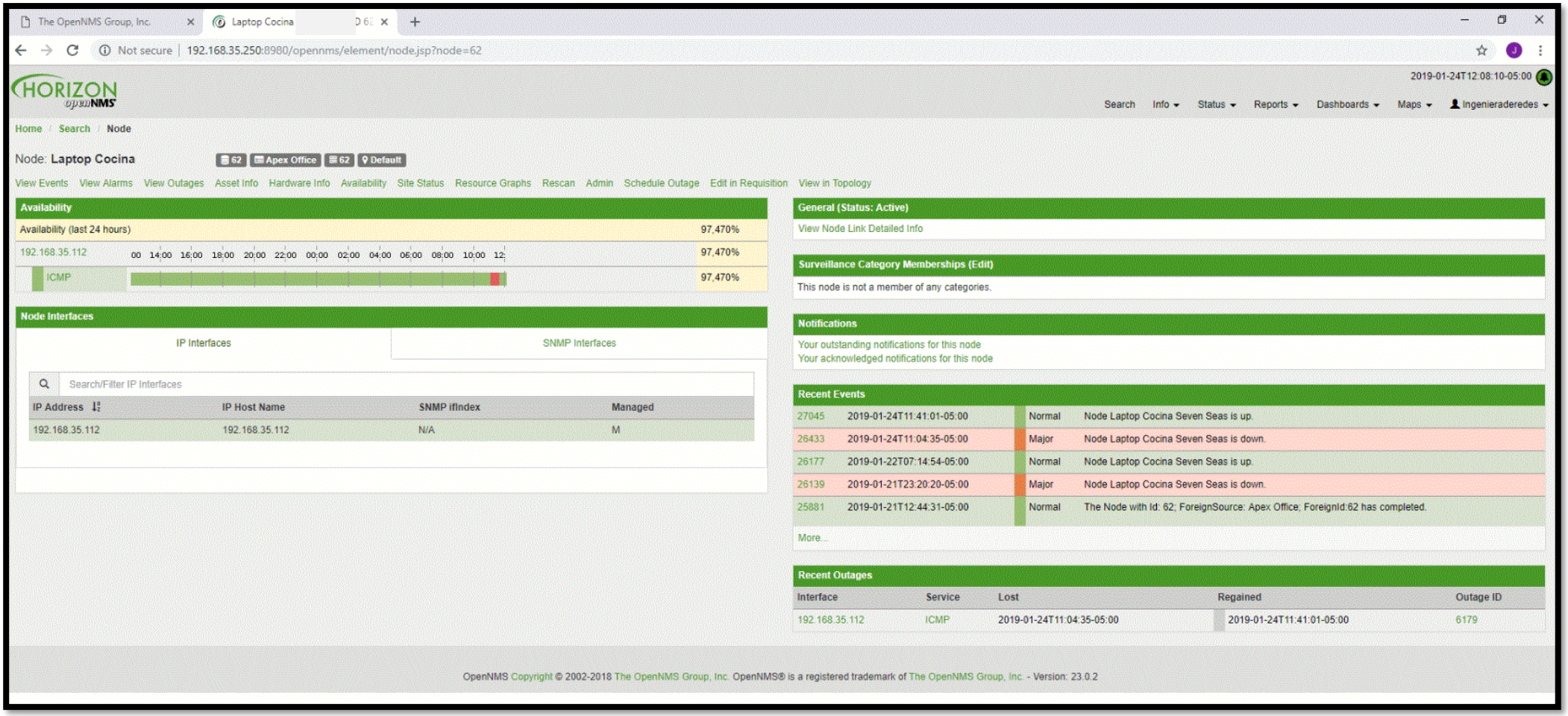


Figura 4.11 Monitoreo de una laptop ubicada en el ambiente de cocina utilizado por la administradora del área
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

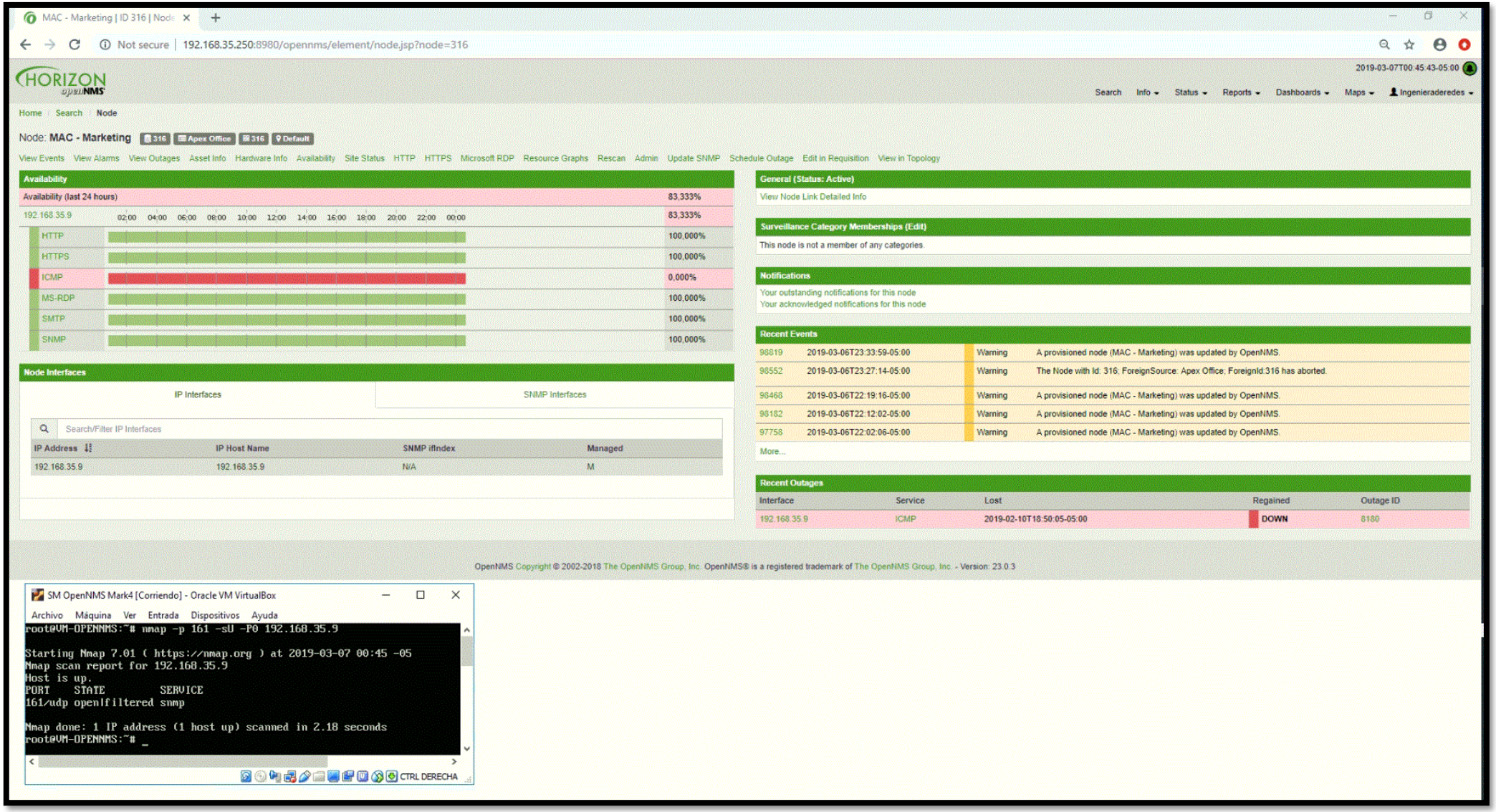


Figura 4.12 Monitoreo de un equipo terminal desktop: PC-Mac del área de Marketing
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

B. Dispositivos monitoreados de las sedes remotas

En las sedes remotas existen equipos de comunicación como routers y switches no administrables, por ello es importante monitorear los routers quienes reciben servicio de internet y datos del ISP para brindar servicio de conectividad de internet y datos a los equipos terminales de las sedes remotas.

Antes de que la empresa migrara de proveedor de internet, el anterior ISP brindaba para cada sede remota dos equipos de comunicación (DBI "servicio de internet" y DBA "servicio de datos"), por lo que en cada sede remota se tenía dos routers de comunicación y para cada equipo de comunicación se brindaba una IP del segmento de red de tienda o sede remota.

Por ello en la figura 4.13 en donde se presenta el monitoreo del equipo de comunicación de la Sede A (sede remota), se observa dos IPs donde una de ellas no está siendo monitoreada ya que tras la migración de proveedor hoy se tiene sólo un equipo de comunicación (router) desde donde se imparte conectividad de internet y datos a todos los equipos terminales de la sede remota. Es decir la IP privada 192.168.195.65 está siendo utilizada para el equipo router de la sede remota y la IP privada 192.168.195.66 no está siendo utilizada puesto que pertenecía al segundo equipo de comunicación que se utilizaba con el anterior ISP.

Se hace uso de la herramienta nmap para comprobar el estado activo del servicio del protocolo SNMP a través del puerto 161 UDP y de acuerdo a la información obtenida se observa que el puerto se encuentra abierto y filtrado.

Finalmente para este caso en particular no se observa eventos de caída de nodo por lo que el funcionamiento del router se encuentra en perfectas condiciones y en el caso hipotético de que se presentaran y la recuperación de estos se diera en breves minutos, por lo general, estos problemas reportados se deben a fallas de tipo eléctrico en el que existe generalmente falso contacto del cable de alimentación del dispositivo de comunicación con el estabilizador.

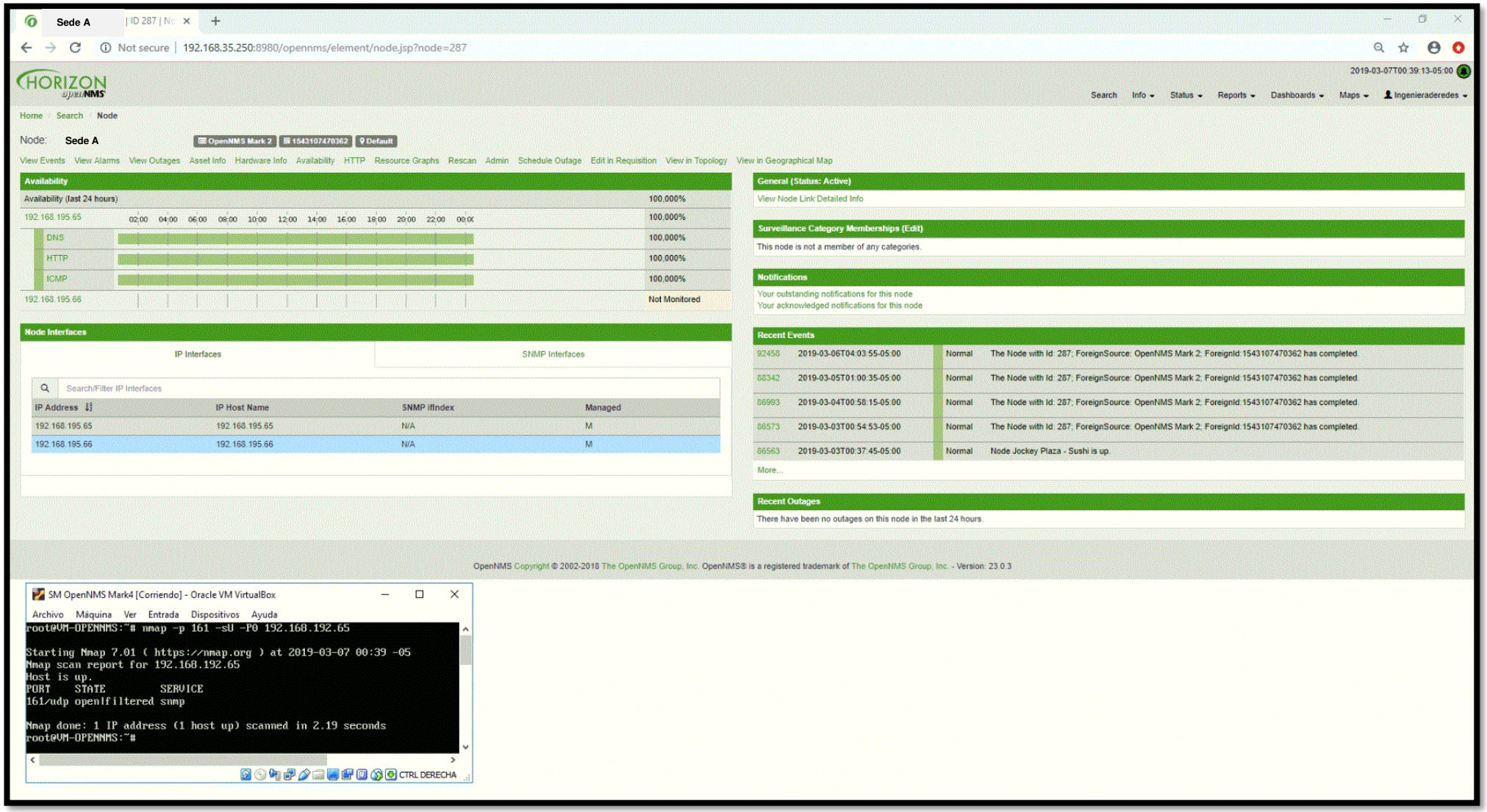


Figura 4.13 Monitoreo del dispositivo de comunicación "router" de una sede remota-Sede A
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

La figura 4.14 corresponde al monitoreo de dos IP privadas correspondientes a dos equipos de comunicación (routers) ubicados en dos tiendas contiguas pertenecientes a la Sede B (sede remota), ambas tiendas hacen uso de un solo segmento de red por ello las IPs privadas 192.168.194.17 y 192.168.194.18 pertenecen a dos equipos routers que brindan servicio de conectividad de internet y de datos a los equipos terminales en la Sede B (sede remota).

Generalmente la empresa emplea segmentos de red diferenciados para las tiendas que pertenecen a una sede remota, sin embargo esta configuración ha sido un caso excepcional.

Se muestra un evento menor en el que se detecta que el uso del protocolo HTTP ha tenido una caída de servicio por un lapso de 26 segundos, posteriormente se muestra un siguiente evento en el que señala que el evento ha sido corregido.

La empresa e-commerce analizada administra un conjunto de cadenas de tiendas de diferentes marcas. La figura 4.15 muestra una de las sedes remotas, Sede C, perteneciente a una de las marcas que administra la empresa e-commerce analizada.

No existe ningún evento de la categoría menor ni mayor por lo que de acuerdo a los eventos mostrados en la figura 4.15 indica que el funcionamiento del equipo de comunicación es correcto.

Esta sede remota anteriormente tenía un servicio de internet contratado diferente al común que se tenía en la mayoría de tiendas o sedes remotas con el anterior ISP; este servicio contratado consistía en utilizar un único equipo de comunicación que brindara únicamente servicio de internet, por lo que la única IP privada monitoreada corresponde al equipo de comunicación utilizado en tienda. En la figura 4.15 se muestra el monitoreo de un dispositivo de comunicación de otra sede remota, Sede C.

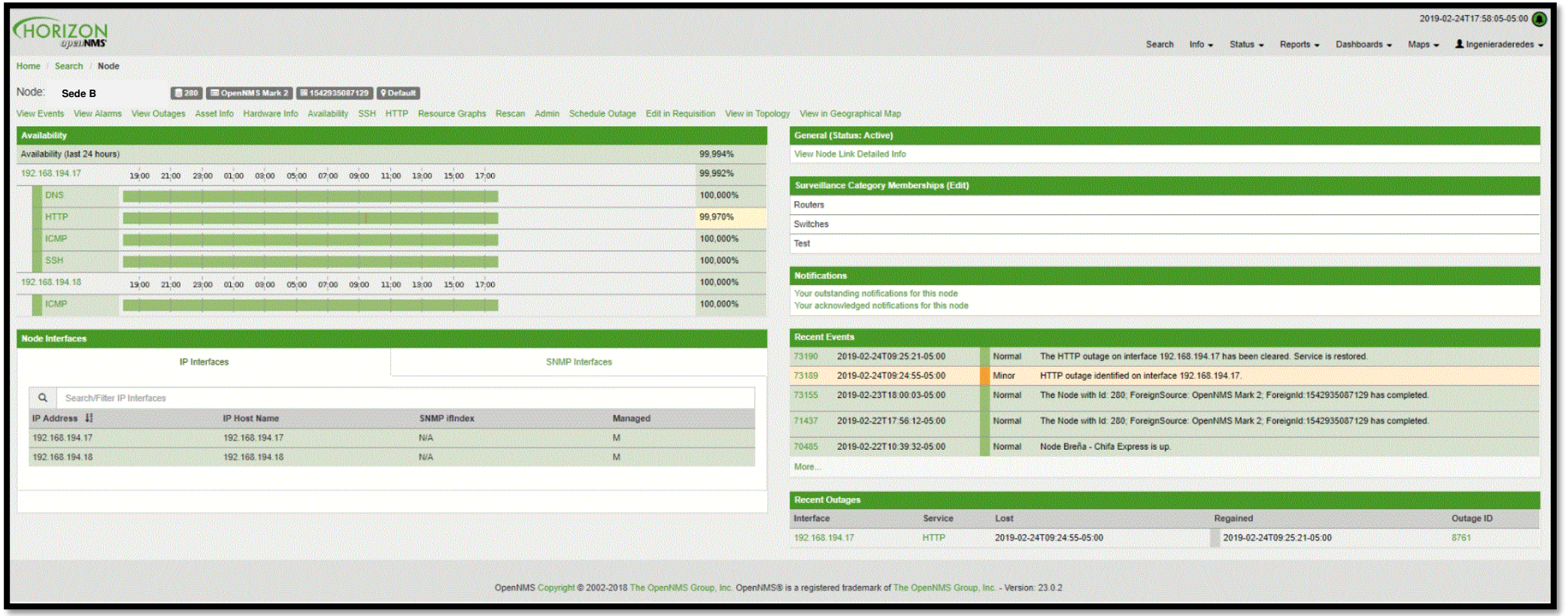


Figura 4.14 Monitoreo de routers de dos tiendas contiguas ubicadas en centro comercial de la Sede B
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

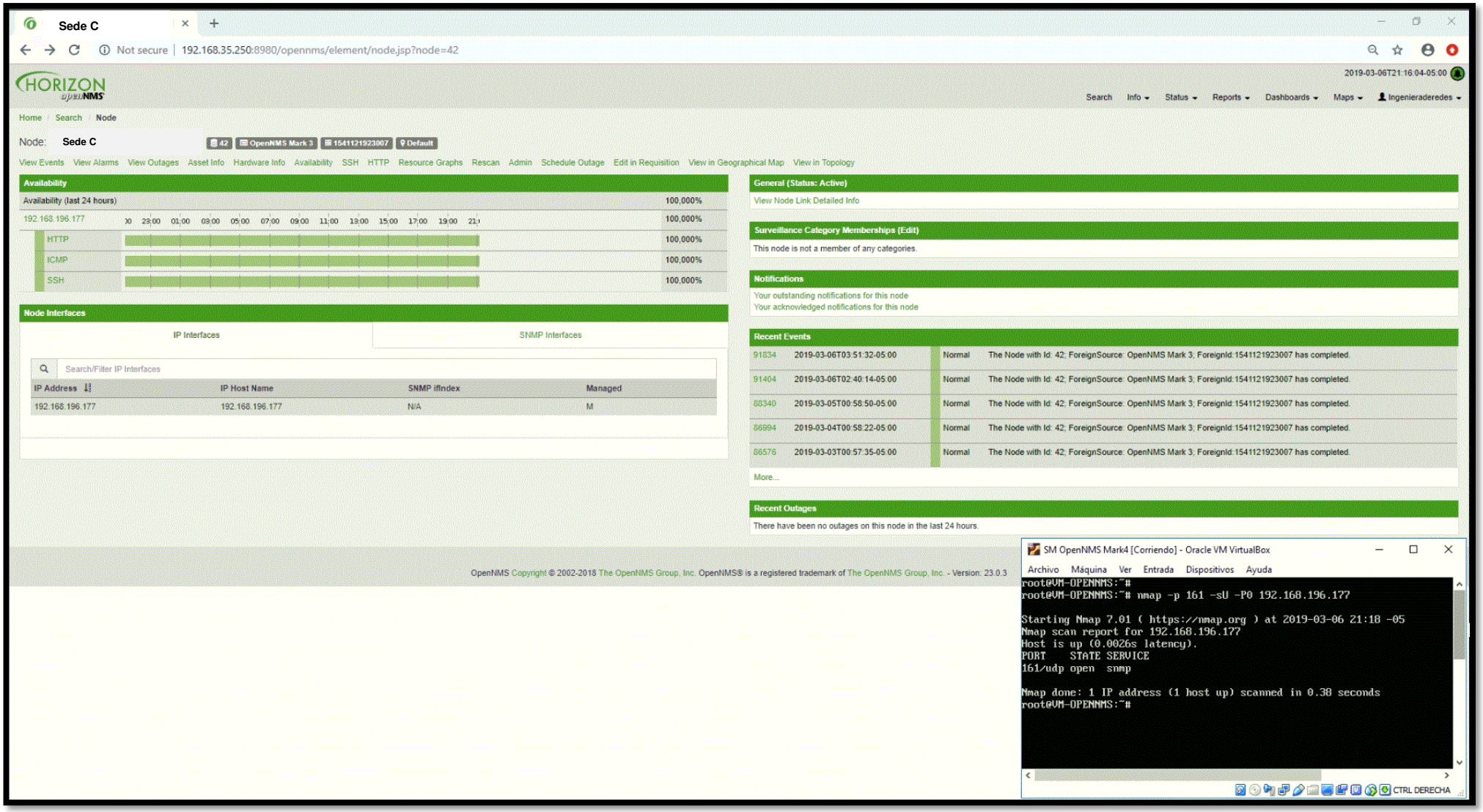


Figura 4.15 Monitoreo de un router ubicado en sede remota (Sede C) de una de las marcas que administra la empresa e-commerce analizada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

4.1.5.1 Gráficos proporcionados por el prototipo de monitoreo

A. Análisis de principales protocolos de comunicación

Cada equipo de comunicación (switches) de la empresa e-commerce analizada brinda datos al prototipo de monitoreo para ser reflejados en gráficos donde se muestra el tiempo de respuesta haciendo uso de los diferentes protocolos, así como el ancho de banda utilizado.

El prototipo de monitoreo de red propuesto puede obtener datos de la transmisión de paquetes de entrada (in), salida (out) así como la retransmisión de paquetes de datos en red; esta información recolectada durante una semana es mostrada a través de una gráfica.

En la figura 4.16 se muestra el monitoreo de un switch de distribución ubicado en un área administrativa de la empresa e-commerce analizada, en la cual se observa el tiempo de respuesta de la transmisión fiable de paquetes de datos sobre la red.

El monitoreo de este dispositivo de comunicación a través del protocolo TCP, es de suma importancia puesto que brinda servicio de conectividad a host que se encuentran operativos (24X7), host destinados al área de operaciones. De acuerdo a la gráfica mostrada en el eje X se muestra la fecha de monitoreo y en el eje Y se muestra el tiempo de respuesta de la transmisión fiable de paquetes en minutos por segundo.

La figura 4.17 corresponde al análisis de datos de la figura 4.16, es decir se muestran los datos de la gráfica en forma numérica ordenados en columnas cuya clasificación es la siguiente: fecha y hora, transmisión de paquetes de entrada, transmisión de paquetes de salida, y las retransmisiones de los paquetes.

Esta información permite tener un control preciso de la transmisión de los paquetes de datos en determinada fecha y hora.

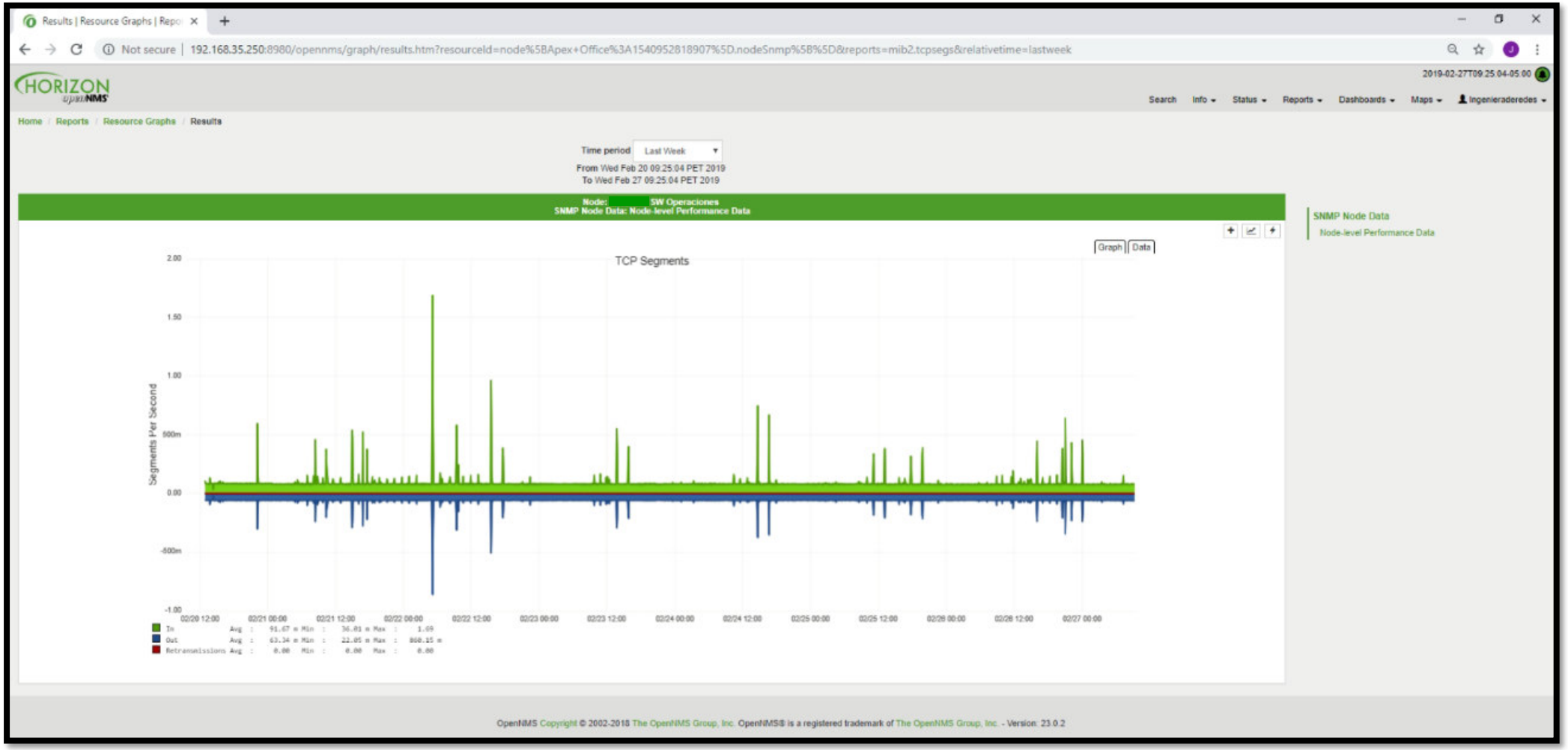


Figura 4.16 Monitoreo de un switch de distribución a través del protocolo TCP
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

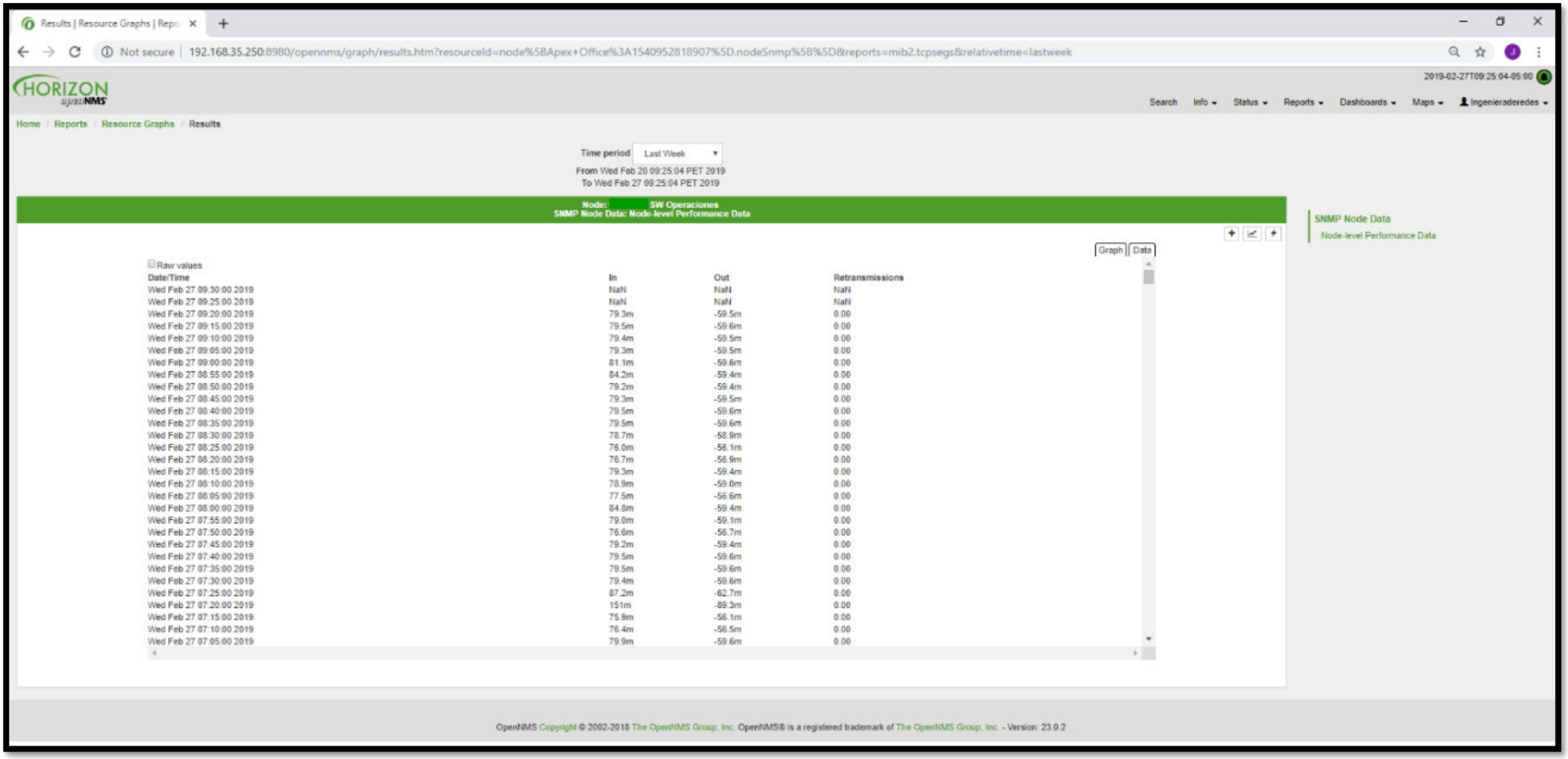


Figura 4.17 Data correspondiente al gráfico de la figura 4.16
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

En la figura 4.18 se puede apreciar que el prototipo de monitoreo de acuerdo a la información recolectada puede pronosticar mediante una gráfica.

La gráfica de la figura 4.18 corresponde al ***pronóstico de la transmisión de datos fiable de entrada*** por un período de 1 mes en delante, de acuerdo a la data recolectada en el monitoreo del dispositivo de comunicación durante una semana, de manera experimental. Los datos pronosticados son una referencia de lo que podría acontecer puesto que el equipo puede presentar fallas físicas u ocurrir alguna otra incidencia.

La figura 4.19 es un gráfico que representa el ***pronóstico de la transmisión de datos fiable de salida*** por un período de 1 mes en delante, de acuerdo a la data recolectada en el monitoreo del dispositivo de comunicación durante una semana, de manera experimental.

En la figura 4.20 se presenta incluso el ***pronóstico en gráfico de la transmisión de paquetes fiables ocurridos durante la retransmisión de datos fiables*** en el equipo de comunicación del área de operaciones, área que labora (24X7).

La figura 4.21 muestra el análisis del monitoreo haciendo uso del protocolo ICMP donde los ejes X, Y indican fecha de monitoreo y tiempo de respuesta basado en minutos por segundo.

Cada gráfica obtenida del prototipo de monitoreo permite obtener información detallada a través de data como se muestra en la figura 4.17 y a través de pronósticos, es decir gráficas que permiten diagnosticar en base a lo analizado durante una semana (tiempo referencial con fines experimentales), como se muestran en las figuras 4.18, 4.19 y 4.20 en la que brindan un pronóstico cuya fecha o período de días a pronosticar el comportamiento de lo analizado en el futuro, puede ser personalizado, además el prototipo de monitoreo brinda fechas exactas para realizar el pronóstico de las gráficas que varían de 1, 7 y 31 días en adelante para mostrar al administrador de red el posible comportamiento del protocolo que desee analizar.

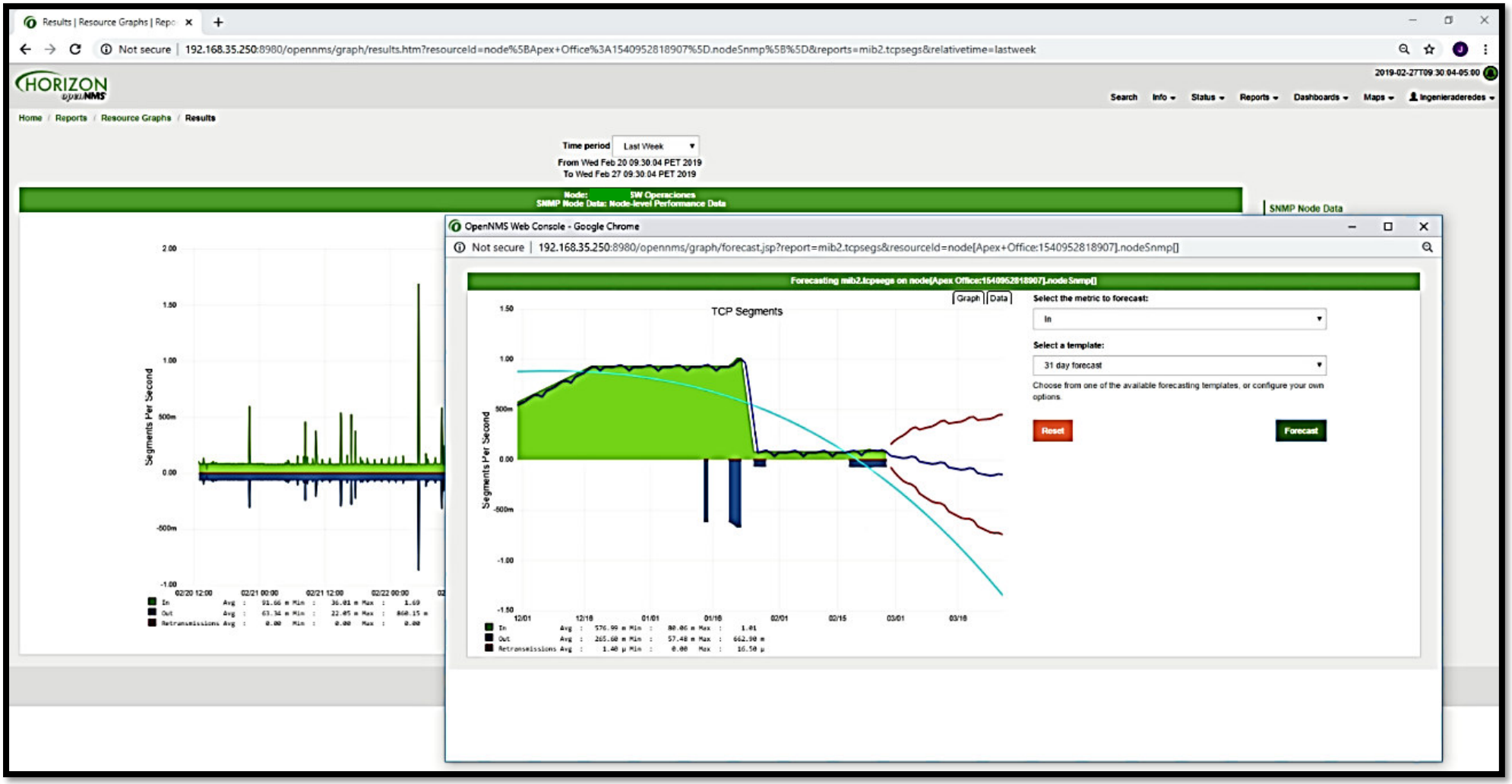


Figura 4.18 Pronóstico de gráfica 4.16 de la transmisión de datos fiable de entrada
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

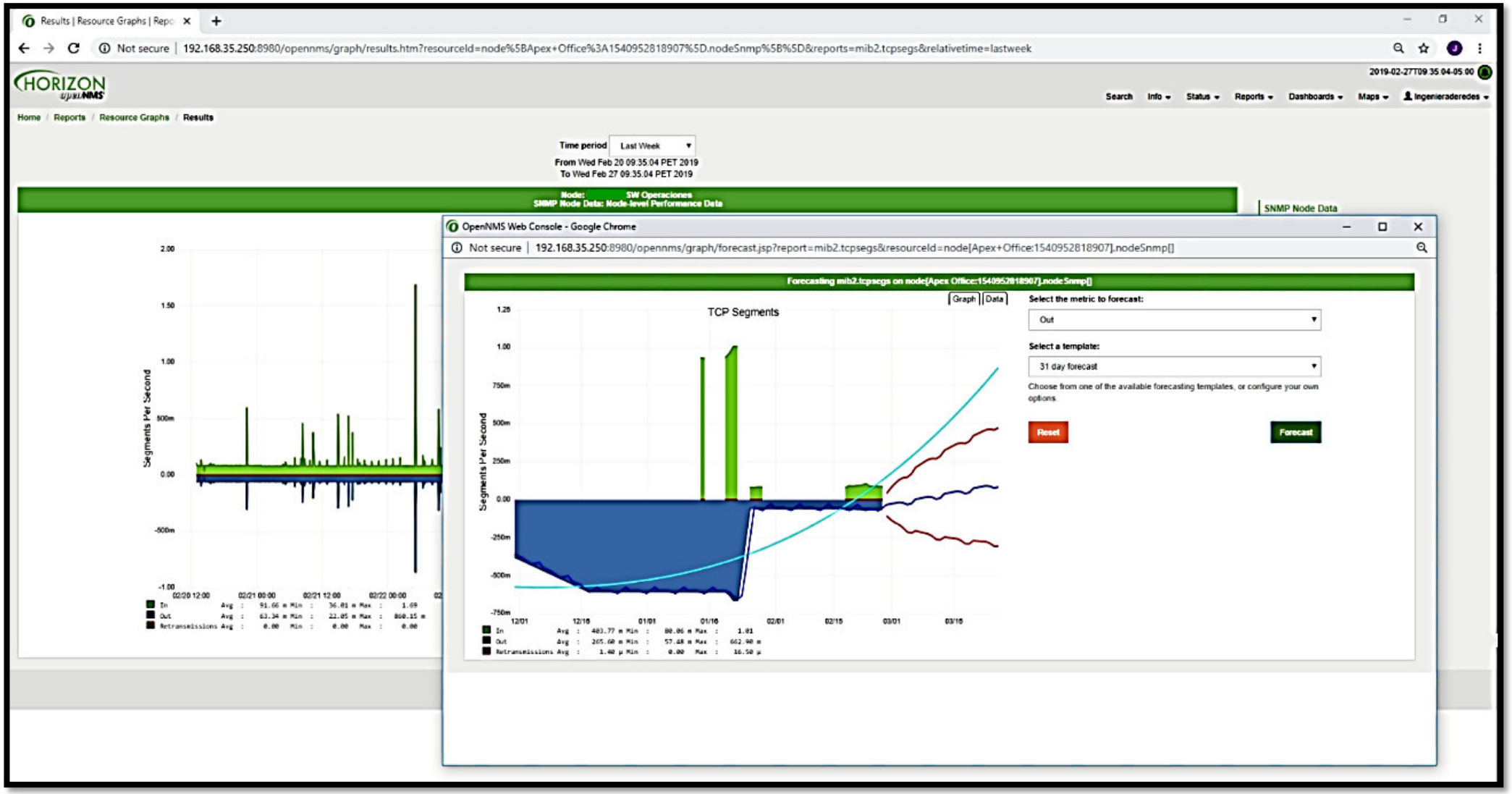


Figura 4.19 Pronóstico de gráfica 4.16 de la transmisión de datos fiable de salida
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

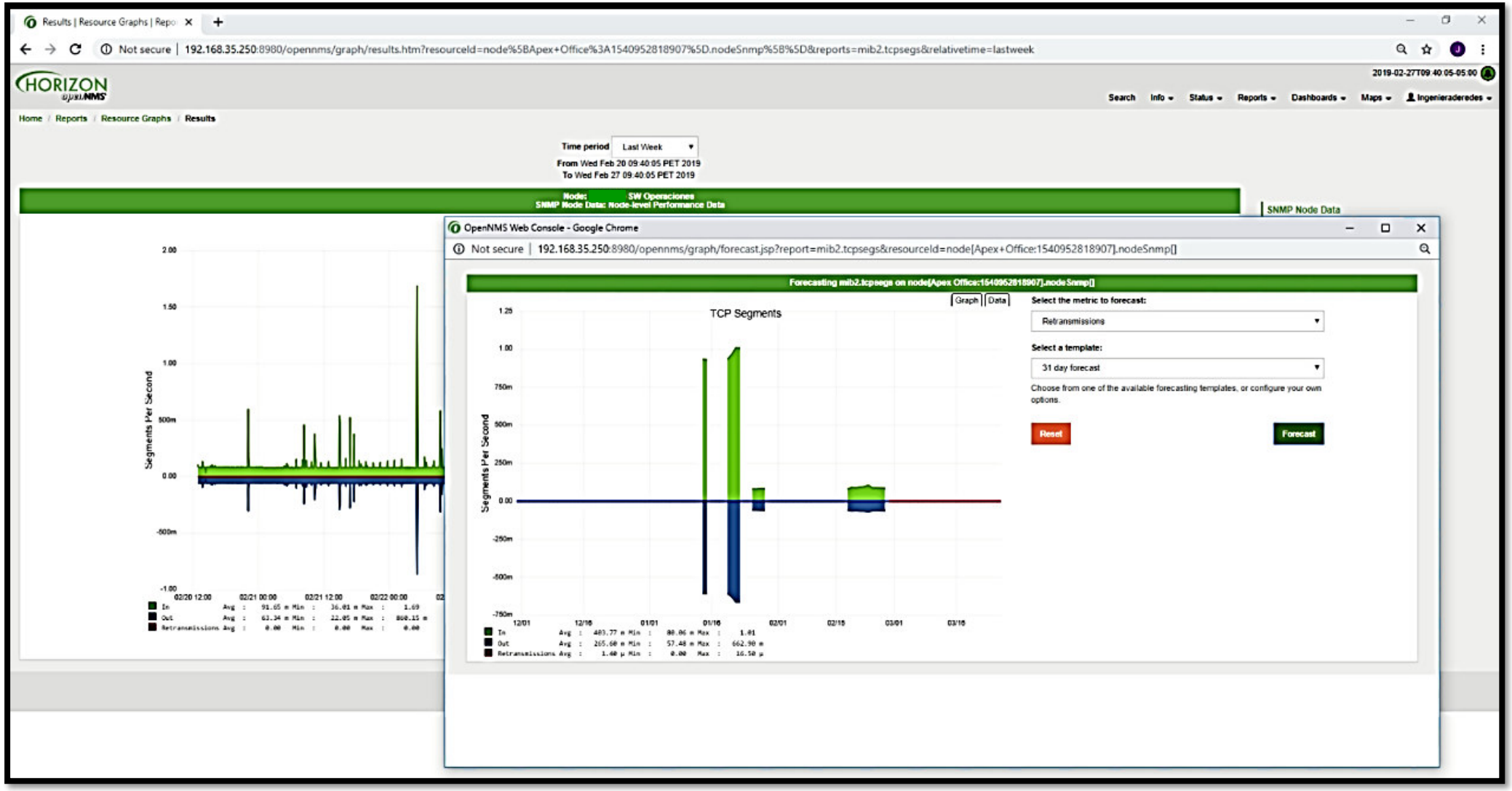


Figura 4.20 Pronóstico de gráfica 4.16 de la retransmisión de datos fiables
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

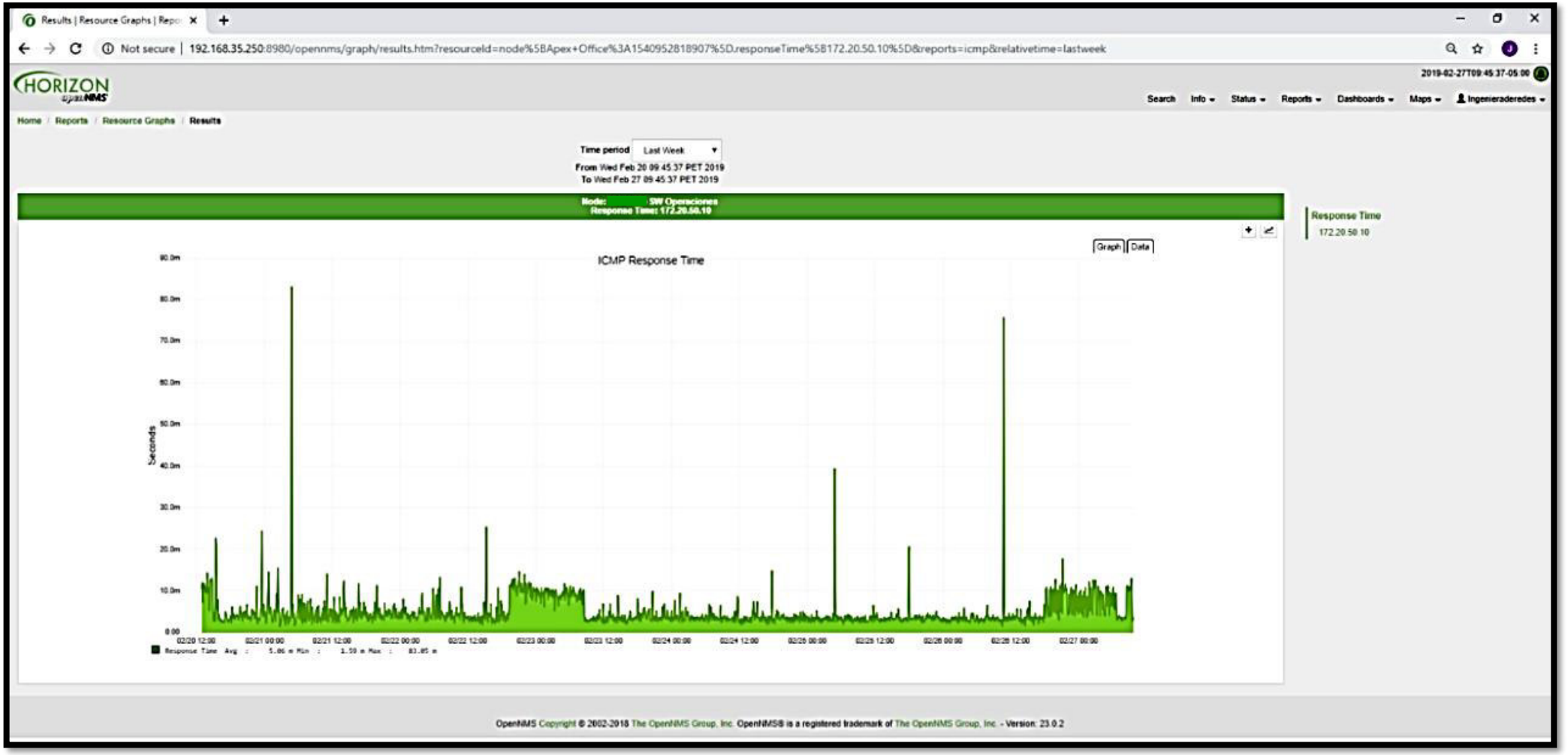


Figura 4.21 Monitoreo de switch del área de operaciones bajo el análisis del protocolo ICMP
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

La figura 4.22 muestra el análisis del monitoreo mediante gráfica, del protocolo HTTP en la que los ejes X, Y indican fecha de monitoreo y tiempo de respuesta en minutos y segundos, respectivamente.

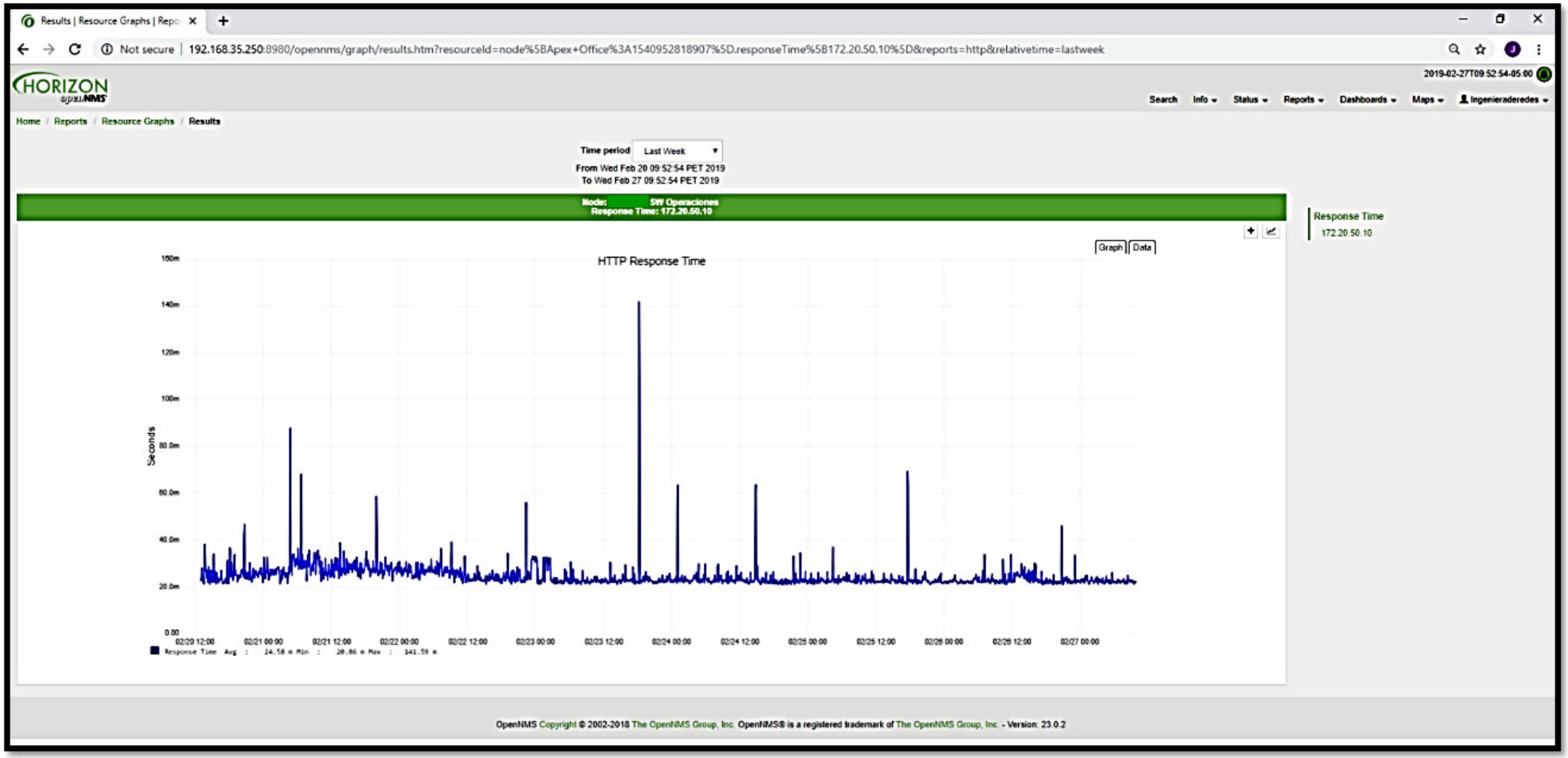


Figura 4.22 Monitoreo del switch de operaciones haciendo uso del protocolo HTTP
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

En la figura 4.23 se observa el monitoreo en gráfica del protocolo HTTPS del equipo de comunicación del área de operaciones.

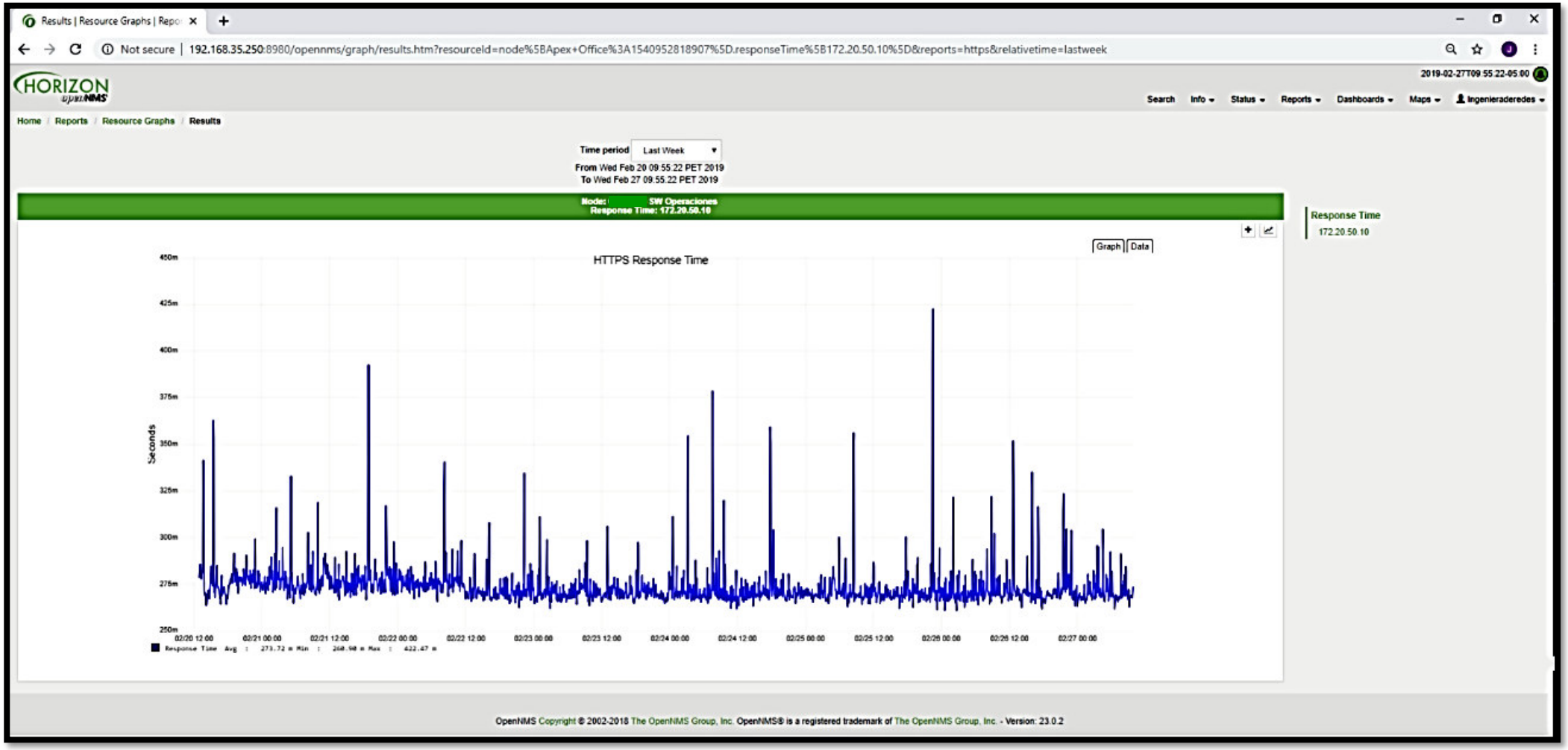


Figura 4.23 Monitoreo del protocolo HTTPS en el Switch del área de operaciones
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

La figura 4.24 corresponde al monitoreo del protocolo SSH del equipo de comunicación ubicado en el área de operaciones que viene siendo analizado.

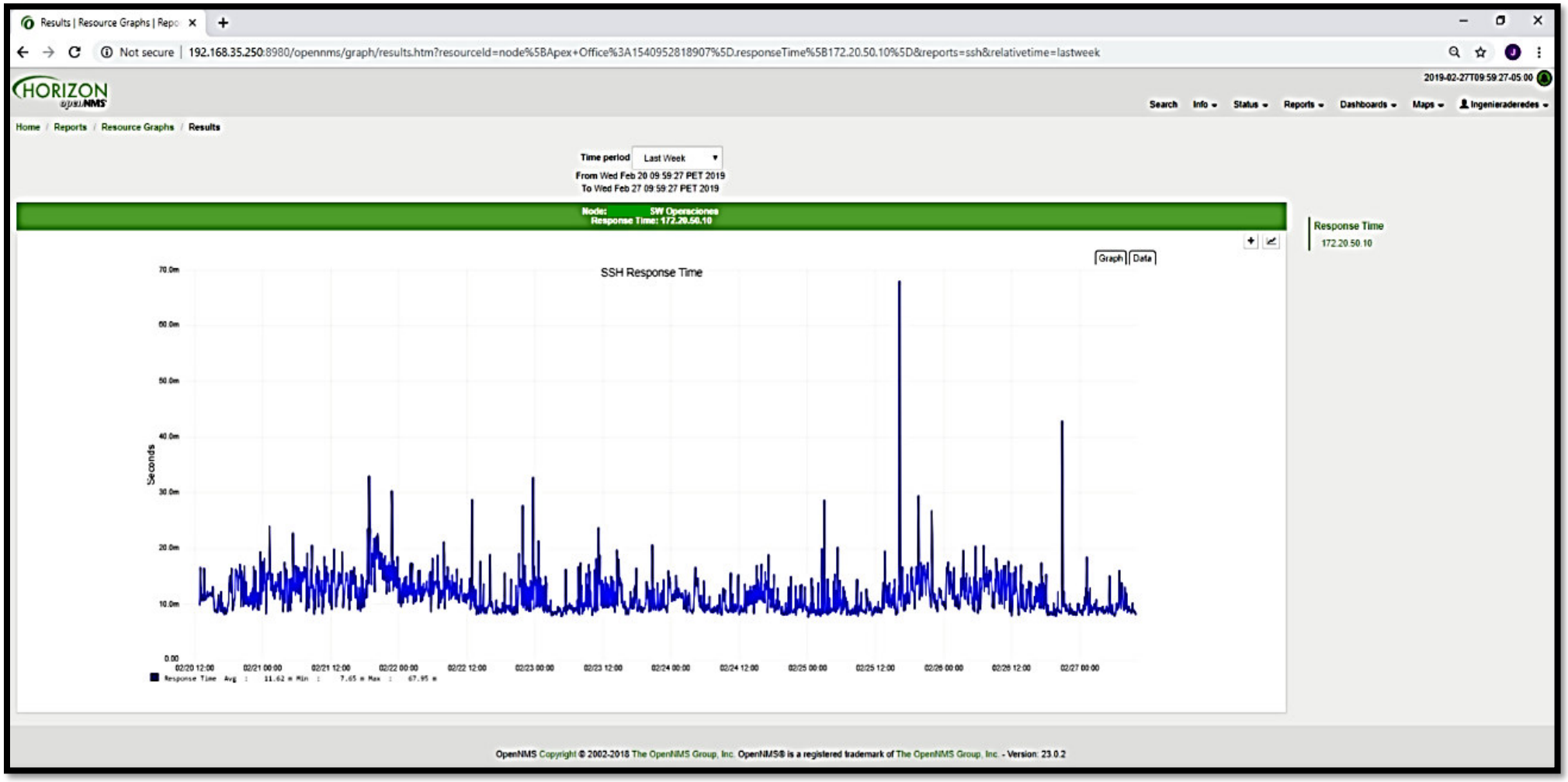


Figura 4.24 Monitoreo del equipo de comunicación analizado previamente y brinda información del protocolo SSH
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

Las figuras anteriormente mostradas han sido analizadas de un mismo equipo de comunicación en la que el tiempo de referencia que se tomó para analizar y/o monitorear los diferentes protocolos diagnosticados en el dispositivo de comunicación es de una semana, tiempo considerado de manera experimental para evaluar los resultados de manera general.

B. Análisis del tráfico o ancho de banda empleado

El prototipo de monitoreo propuesto permite monitorear el tráfico utilizado a través de dos gráficas: bits (in/out) y traffic utilization (in/out) ambos medidos por la unidad de Gbps.

La figura 4.25 muestra la gráfica de bits (in/out) de un equipo de comunicación utilizado en el área de Tecnologías de la Información (TI).

En la figura 4.26 se observa el gráfico del tráfico utilizado (in/out) del mismo equipo de comunicación analizado en la figura 4.25. La figura 4.26 analiza el tráfico utilizado por los usuarios (personal administrativo) del área de tecnologías de la información (TI), área que realiza un mayor consumo puesto que constantemente hace uso de múltiples recursos, como el área de desarrollo por ejemplo cuando realizan descarga y carga masiva de datos correspondiente a las bases de datos.

Además, este equipo de comunicación en particular alberga una gran cantidad de usuarios en la subred LAN1-VLAN5, subred que sirve de consulta a otras redes para llegar a ambientes de producción donde se encuentran almacenados localmente algunos repositorios de ciertos aplicativos propios de la empresa e-commerce analizada.

El análisis a través de gráfico del monitoreo de los diferentes equipos de comunicación permite tener una visualización completa de los recursos que vienen siendo utilizados por los usuarios de la empresa, es decir por el consumo que realiza el personal administrativo. Estos resultados permiten al administrador de red tomar una decisión eficaz y oportuna para resolver inconsistencias y/o inconvenientes presentados en el desempeño de las labores ocurridos día tras día en la empresa e-commerce analizada.

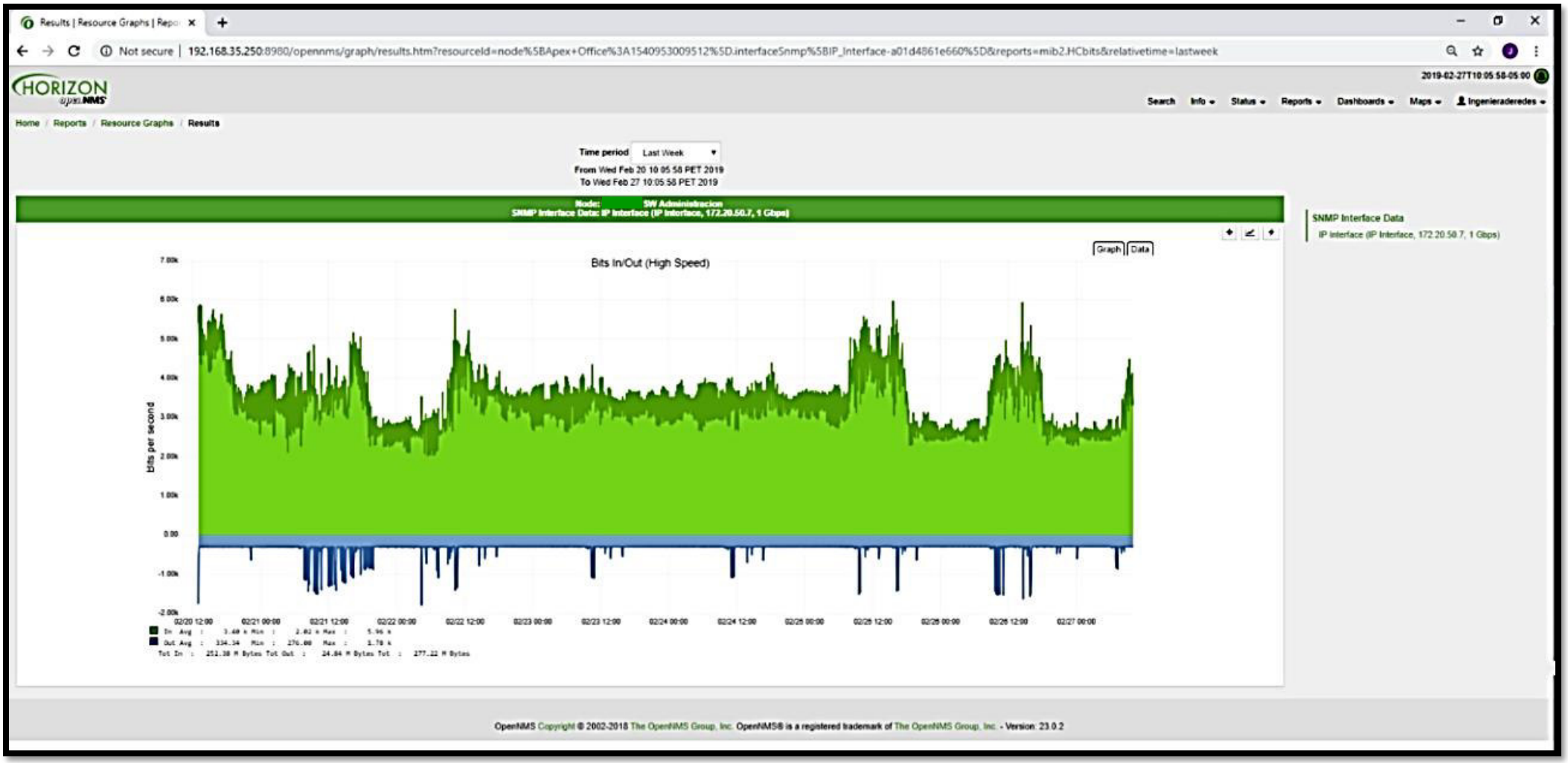


Figura 4.25 Monitoreo de los bits (in/out) del switch de nombre administración que brinda servicio de conectividad de internet al área de TI
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

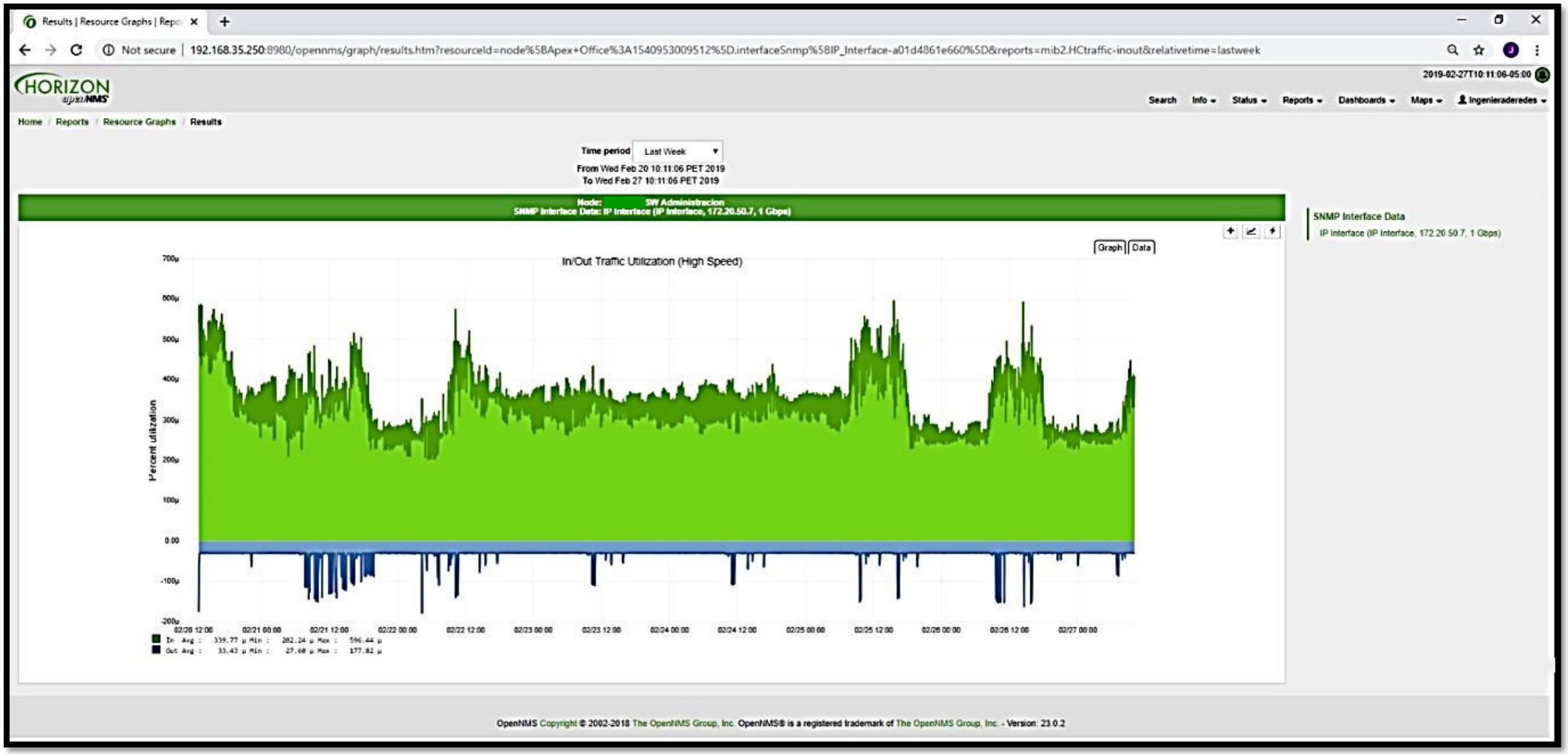


Figura 4.26 Monitoreo del tráfico utilizado, analizado del equipo de comunicación del área de TI
[Elaboración propia basado en el prototipo de monitoreo de red propuesto]

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

a.- A través del análisis de diferentes sistemas de monitoreo estudiados a lo largo de la investigación del presente proyecto de tesis y gracias a la experiencia obtenida en la administración de sistemas de monitoreo licenciados, se puede afirmar que los sistemas licenciados, si bien son muy útiles para las empresas, no son la única herramienta de monitoreo que brindan resultados eficaces en tiempo real.

La presente propuesta de prototipo de monitoreo opensource, cumple con las funciones que realiza un sistema de monitoreo licenciado. Además es un prototipo altamente personalizable que no sólo monitorea equipos o dispositivos de comunicación y de usuarios finales de una sede sino que también permite monitorear diferentes enlaces o sedes remotas de una determinada empresa, sedes remotas ubicadas correctamente dentro de un plano con las direcciones correspondientes de cada una de las sedes remotas.

El presente proyecto de tesis ha permitido realizar una investigación exhaustiva de un sistema operativo no comúnmente utilizado en el monitoreo de redes de datos (sistema operativo Linux), así como de las herramientas que se ha requerido para la captura de datos en la red y en tiempo real.

b.- Gracias al análisis y estudio del protocolo simple de administración de red, SNMP, se ha propuesto en este proyecto de tesis, el presente prototipo de monitoreo basado en las necesidades propias de una empresa e-Commerce real, descrita en el desarrollo de la tesis que ha contribuido en mejorar los tiempos de respuesta ante incidentes de la red de datos de la empresa e-Commerce analizada.

Este prototipo de monitoreo ha permitido analizar los diferentes dispositivos de comunicación y dispositivos terminales de la red de datos de la empresa e-Commerce real, indicando si se encuentran activos o existe alguna anomalía en su funcionamiento; por ello ha quedado demostrado que la eficiencia en el uso de una herramienta no licenciada es igual de competente que una herramienta licenciada, siendo aún un prototipo de monitoreo, no es un sistema de monitoreo como tal, en la que de manera estándar se encuentran instalados en los servidores de la empresa que monitorearán.

c.- El prototipo de monitoreo ha sido implementado en la empresa e-Commerce analizada, presentándose los datos recolectados y mostrados en el capítulo 4, denominado Resultados, donde se explica detalladamente la funcionalidad de este prototipo de monitoreo.

5.2 RECOMENDACIONES

Este proyecto de tesis tiene una segunda versión y hasta tercera porque como bien se mencionó en anteriores capítulos, OpenNMS herramienta opensource base del prototipo de monitoreo tiene dos versiones: Horizon y Meridian.

La versión Meridian de OpenNMS es una versión enterprise que la empresa e-commerce analizada puede hacer uso si lo requiere. En el futuro, el desarrollo de un sistema de monitoreo haciendo uso de OpenNMS bajo la versión de Meridian implementado en los servidores de la empresa, sería una interesante propuesta de tesis a desarrollar.

Actualmente, los proveedores de Internet ya empiezan a planificar el uso de las nuevas tecnologías emergentes como Redes Definidas por Software-SDN. Estas nuevas redes requerirán el monitoreo y gestión de sus componentes; siendo esta una nueva oportunidad de profundizar la investigación y desarrollo de tesis de estos temas en SDN.

El presente proyecto de tesis recomienda que los principales centros de investigación del país, deben poner en práctica estas nuevas tecnologías emergentes como son las Redes Definidas por Software-SDN, partiendo del Instituto de Investigación de la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos (U.N.M.S.M.) en coordinación conjunta con los programas realizados por el Vicerrectorado de Investigación y Posgrado para promover el cambio desde la arquitectura de la red de datos de la Red Telemática de la U.N.M.S.M.

Las Redes Definidas por Software son temas tratados hoy en día por las grandes y prestigiosas universidades como Stanford y Universidad Carlos III de Madrid, colocándolos a la vanguardia en el ámbito de las nuevas tecnologías emergentes de redes de datos lo cual es digno de admirar e imitar poniendo en práctica en la Decana de América, la Universidad del Perú, la Universidad Nacional Mayor de San Marcos.

ANEXO I

Matriz de Consistencia

TÍTULO: "Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce"				
PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES**	**METODOLOGÍA**
Problema General: ¿Cómo mejorar los tiempos de respuesta ante incidentes en una red de datos de una empresa e-Commerce?	**Objetivo General:** Implementar un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basado en software libre para una empresa e-Commerce.	**Hipótesis General:** Utilizando el protocolo SNMP se implementará un prototipo de monitoreo de dispositivos de comunicación y usuarios finales basado en software libre para una empresa e-Commerce.	**Variables independientes:** Herramientas de monitoreo de software licenciado, herramientas de monitoreo de software no licenciado, herramientas de monitoreo de gestión en la nube, protocolo de administración de red SNMP, herramienta NMAP y la arquitectura del prototipo de monitoreo de redes de datos. **Variable dependiente:** Prototipo de monitoreo de redes de datos propuesto para la empresa e-Commerce analizada.	**Tipo de investigación:** Experimental. - Análisis del efecto producido en la manipulación de variables independientes sobre variables dependientes. **Diseño de la investigación:** ✓ Recopilación de documenta-ción técnica para el análisis de los diferentes sistemas de monitoreo de redes de datos. ✓ Identificación de una empresa que brinda servicios por internet en la que se propone una arquitectura de prototipo de sistema de monitoreo. ✓ Implementa-ción de un prototipo de
Problemas específicos: ¿Cómo proponer nuevas soluciones personalizadas?	**Objetivos específicos:** Analizar y comparar los diferentes sistemas de monitoreo de dispositivos de comunicación y usuarios finales.	**Hipótesis específicas:** Analizando y comparando los diferentes sistemas de monitoreo de los dispositivos de comunicación y usuarios finales se podrá proponer nuevas soluciones personalizadas.		
Problemas específicos: ¿Cómo elaborar un prototipo de	**Objetivos específicos:** Analizar el protocolo SNMP y	**Hipótesis específicas:** Analizando el protocolo SNMP se		

un sistema de monitoreo de dispositivos de comunicación y usuarios finales aplicado a una empresa e-Commerce?	elaborar un prototipo de sistema de monitoreo de dispositivos de comunicación y usuarios finales aplicado a una empresa e-Commerce.	podrá implementar un sistema de monitoreo de dispositivos de comunicación y usuarios finales aplicado a una empresa e-Commerce.		sistema de monitoreo propuesto.
Problemas específicos: ¿Es posible implementar el prototipo propuesto para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP aplicado a una empresa e-Commerce usando software libre?	**Objetivos específicos:** Implementar el prototipo propuesto para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP aplicado a una empresa e-Commerce usando software libre.	**Hipótesis específicas:** Es posible implementar el prototipo propuesto para el monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP aplicado a una empresa e-Commerce usando software libre.		

ANEXO II

Comandos para instalar Prototipo de Monitoreo

1.- PROTOTIPO DE MONITOREO (SERVIDOR VIRTUAL)

a. Prerrequisitos

- Un servidor que ejecuta Ubuntu 16.04.
- Un usuario no root con privilegios sudo configurados en el servidor.
- Una configuración de dirección IP estática xxx.xxx.xxx.xxx en el servidor.

b. Inicio

b.1 Actualizar el sistema a la última versión estable. Ejecutar los siguientes comandos:
sudo apt-get update -y
sudo apt-get upgrade –y

b.2 Después de actualizar el sistema, establecer un nombre de dominio completo y adecuado. Editar el archivo / etc / hosts:
sudo nano /etc/hosts

Añadir la siguiente línea:
xxx.xxx.xxx.xxx server.opennms.local server

A continuación, abrir el archivo / etc / hostname:
sudo nano /etc/hostname

Añadir la siguiente línea:
server.opennms.local

Guardar el archivo cuando haya terminado, luego reiniciar el sistema para aplicar estos cambios.
sudo systemctl restart postgresql
sudo systemctl enable postgresql

Una vez que haya terminado, proceder a instalar Java.

c. Instalar Java

OpenNMS no es compatible con Java 8 todavía. Se recomienda utilizar Java 7. Para instalar Java 7, deberá agregar PPA a la lista de fuentes de apt. Ejecutar el siguiente comando:
sudo add-apt-repository ppa:webupd8team/java

A continuación, actualizar el repositorio ejecutando el comando:
sudo apt-get update -y

Luego de actualizarse el repositorio, instalar Java 7 simplemente ejecutando el siguiente comando:
sudo apt-get install oracle-java7-installer -y

Verificar la versión de Java con el siguiente comando:
sudo jave -version

Observar el siguiente resultado:
versión java "1.7.0_101"
Java (TM) SE Runtime Environment (compilación 1.7.0_101-b13)
VM de servidor de 64 bits de Java HotSpot (TM) (compilación 25.101-b13, modo mixto)

Una vez terminado, continuar con el siguiente paso.

d. Instalar OpenNMS

Por defecto, OpenNMS no está disponible en el repositorio predeterminado de Ubuntu. Por lo tanto, agregar el repositorio OpenNMS al directorio /etc/apt/sources.list.d. Ejecutar el siguiente comando:
sudo nano /etc/apt/sources.list.d/opennms.list

Añadir las siguientes líneas:
deb http://debian.opennms.org estable principal
deb-src http://debian.opennms.org estable main

Guardar el archivo cuando haya terminado, luego agregar la clave OpenNMS con el siguiente comando:
wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -

Actualizar las listas de repositorios usando el comando:
sudo apt-get update -y

Luego que el repositorio esté actualizado, instalar OpenNMS ejecutando el comando:
sudo apt-get install default-mta opennms -y

Instalado OpenNMS, crear una base de datos para OpenNMS. Ejecutar el siguiente comando:
sudo /usr/share/opennms/bin/install -dis

Observar el siguiente resultado:
Instalador de OpenNMS
==========
==========
Configura tablas, usuarios y otras configuraciones misceláneas de PostgreSQL.
.
.
.
- Ejecución de la fase posterior a la ejecución.
Eliminando la copia de seguridad /usr/share/opennms/etc/discovery-configuration.xml.zip
Terminado en 0 segundos

Finalmente, iniciar el servicio OpenNMS con el siguiente comando:
sudo systemctl start opennms

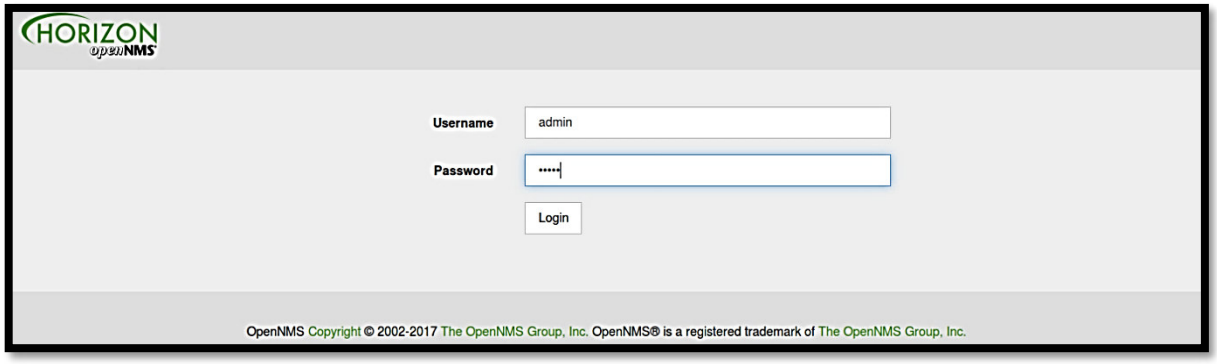
e. Acceso a OpenNMS

De manera predeterminada, OpenNMS se ejecuta en el puerto 8980. Por lo tanto, permitir el puerto 8980 a través del firewall UFW. Por defecto, UFW está deshabilitado en el sistema, por lo que primero se debe habilitar. Habilitarlo con el siguiente comando:
sudo ufw enable

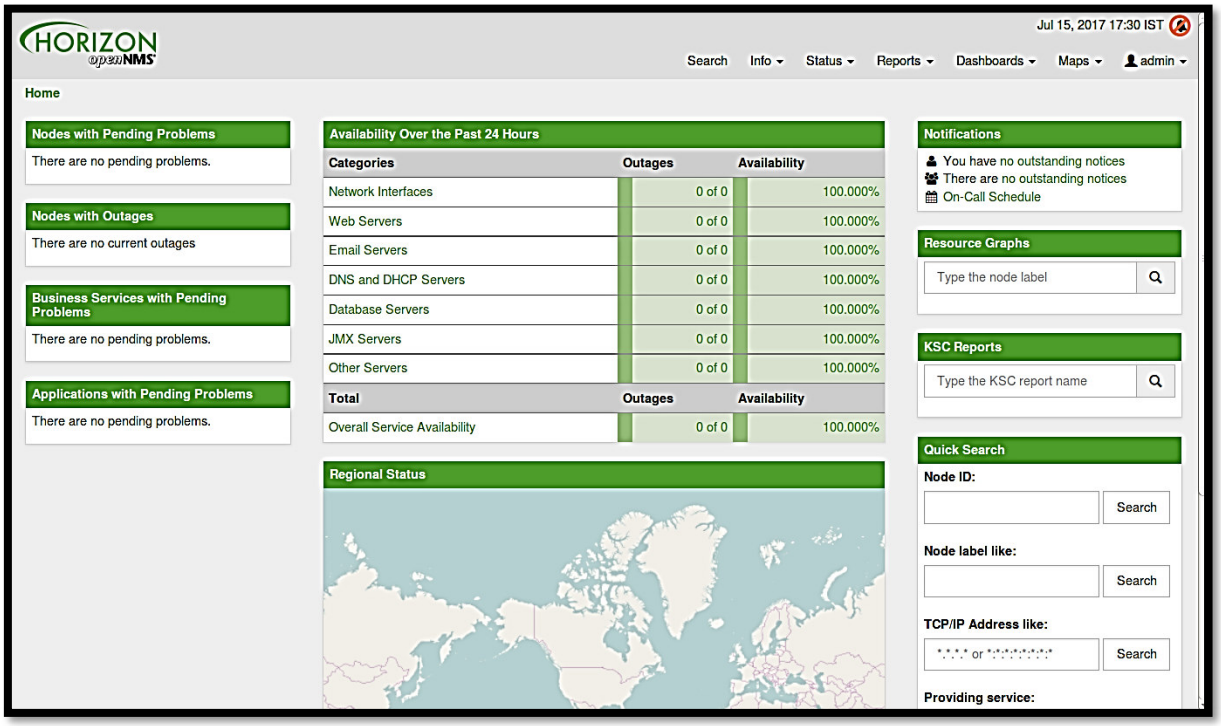
Una vez que el firewall UFW esté habilitado, permitir el puerto 8980 ejecutando el siguiente comando:
sudo ufw allow 8980

Verificar el estado del firewall UFW ejecutando el siguiente comando:
sudo ufw status

Una vez que el firewall UFW esté configurado, abrir el navegador web y escribir la URL **http://xxx.xxx.xxx.xxx:8980/opennms**, debería ver la siguiente pantalla:



Al iniciar sesión con el nombre de usuario " **admin** " y la contraseña " **admin** ", debería ver la siguiente pantalla: A partir de esta pantalla el estudiante y/o profesional puede iniciar con la creación y personalización de la red que desea monitorear.



2.- CONFIGURACIÓN DE HERRAMIENTAS DE MONITOREO EN SERVIDOR VIRTUAL DEL PROTOTIPO DE MONITOREO

a. Configuración CAPSD:

Indica al software del prototipo de monitoreo que busque el agente SNMP que ha configurado. Agregar la siguiente configuración a **capsd-configuration.xml**, reiniciar OpenNMS y volver a escanear los servicios del host mediante la interfaz web. Se debe ver un nuevo servicio **'SNMP-JVM'** en el host.

Configuración en el archivo capsd-configuration.xml

```
<protocol-plugin protocol = "SNMP-JVM" class-name =
"org.opennms.netmgt.capsd.plugins.SnmpPlugin"
                  scan = "on" definido por el usuario =
"false">
    <propiedad key = "timeout" value = "5000" />
    <propiedad clave = "reintentar" valor = "3" />
    <propiedad clave = "puerto" valor = "1161" />
    <propiedad key = "vbname" value = ".
1.3.6.1.4.1.42.2.145.3.163.1.1.4.1" />
</protocol-plugin>
```

b. Configuración de recopilación:

Para indicar al software del prototipo de monitoreo que realmente recopile los datos de este servicio, debe agregar lo siguiente al archivo **collectd-configuration.xml**.

```
<service name = "SNMP-JVM" interval = "300000" user-
defined = "false" status = "on">
    <parámetro clave = "colección" valor = "jvm" />
    <tecla de parámetro = valor "puerto" = "1161" />
    <tecla de parámetro = "reintentar" valor = "3" />
    <tecla de parámetro = valor "tiempo de espera" =
"3000" />
    <tecla de parámetro = "oid" valor = ".
1.3.6.1.4.1.42.2.145.3.163.1.1.4.1" />
</service>
```

c. Creando gráficas:

Editar el archivo de configuración **snmp-graph.properties** y volver a cargar la página de gráficos.

```
report.jvm.heap.name = JVM Heap Memory
report.jvm.heap.columns = jvmHeapUsed, jvmHeapCommitted,
jvmHeapMax
```

```
report.jvm.heap.type = nodeSnmp
report.jvm.heap.command = - title = "JVM Heap Memory" \
 DEF: used = {rrd1}: jvmHeapUsed: AVERAGE \
 DEF: comm = {rrd2}: jvmHeapCommitted: AVERAGE \
 DEF: max = {rrd3}: jvmHeapMax: AVERAGE \
 ÁREA: usado # 0000ff: "usado" \
 GPRINT: usado: MEDIA: "Avg \\:% 5.2lf% s" \
 GPRINT: usado: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: usado: MAX: "Max \\:% 5.2lf% s \\ n" \
 LINE2: comm # 00ff00: "Committed" \
 GPRINT: comm: AVERAGE: "Avg \\:% 5.2lf% s" \
 GPRINT: comm: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: comm: MAX: "Max \\:% 5.2lf% s \\ n" \
 LINE2: max # ff0000: "Max" \
 GPRINT: max: PROMEDIO: "Avg \\:% 5.2lf% s" \
 GPRINT: max: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: max: MAX: "Max \\:% 5.2lf% s \\ n"

report.jvm.nonheap.name = JVM Non-Heap Memory
report.jvm.nonheap.columns = jvmNonHeapUsed,
jvmNonHeapCommitted, jvmNonHeapMax
report.jvm.nonheap.type = nodeSnmp
report.jvm.nonheap.command = - title = "JVM Non-Heap
Memory" \
 DEF: used = {rrd1}: jvmNonHeapUsed: AVERAGE \
 DEF: comm = {rrd2}: jvmNonHeapCommitted: AVERAGE \
 DEF: max = {rrd3}: jvmNonHeapMax: AVERAGE \
 ÁREA: usado # 0000ff: "usado" \
 GPRINT: usado: MEDIA: "Avg \\:% 5.2lf% s" \
 GPRINT: usado: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: usado: MAX: "Max \\:% 5.2lf% s \\ n" \
 LINE2: comm # 00ff00: "Committed" \
 GPRINT: comm: AVERAGE: "Avg \\:% 5.2lf% s" \
 GPRINT: comm: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: comm: MAX: "Max \\:% 5.2lf% s \\ n" \
 LINE2: max # ff0000: "Max" \
 GPRINT: max: PROMEDIO: "Avg \\:% 5.2lf% s" \
 GPRINT: max: MIN: "Min \\:% 5.2lf% s" \
 GPRINT: max: MAX: "Max \\:% 5.2lf% s \\ n"

report.jvm.threads.name = JVM Threads
report.jvm.threads.columns = jvmThreadCount
report.jvm.threads.type = nodeSnmp
report.jvm.threads.command = - title = "JVM Thread Count"
\
 DEF: threads = {rrd1}: jvmThreadCount: AVERAGE \
 LINE2: hilos # 0000ff: "Temas" \
 GPRINT: hilos: PROMEDIO: "Avg \\:% 8.2lf% s" \
 GPRINT: hilos: MIN: "Min \\:% 8.2lf% s" \
 GPRINT: hilos: MAX: "Max \\:% 8.2lf% s \\ n"
```

ANEXO III

RFCs

SNMPv1 RFC

RFC 1157. Protocolo Simple de Manejo de Red.

Las RFC SMIv1 también se aplican a todas las entidades SNMPv1.

Las RFC de MIB-II también se aplican a todas las entidades de agente SNMPv1.

SNMPv2 RFC

Las RFC de la versión 2 de SNMP son:

RFC 1901. Introducción al SNMPv2 basado en la comunidad.

RFC 1908. Coexistencia entre la versión 1 y la versión 2 del marco de administración de red estándar de Internet.

RFC 3416. Versión 2 de las operaciones del protocolo SNMP.

RFC 3417. Asignaciones de transporte.

Las RFC SMIv1 y SMIv2 también se aplican a todas las entidades SNMPv2c.

Las RFC MIB-II también se aplican a todas las entidades de agente SNMPv2c.

SNMPv3 RFC

Las RFC de la versión 3 de SNMP son:

RFC 3410. Introducción y declaraciones de aplicabilidad para el marco de gestión estándar de Internet.

RFC 3411. Una arquitectura para describir los marcos de administración SNMP.

RFC 3412. Procesamiento de mensajes y despacho.

RFC 3413. Aplicaciones SNMP.

RFC 3414. Modelo de seguridad basado en el usuario.

RFC 3415. Modelo de control de acceso basado en vistas.

RFC 3416. Versión 2 de las operaciones del protocolo SNMP.

RFC 3417. Asignaciones de transporte.

RFC 3584. Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet.

RFC 3826. El algoritmo de cifrado del estándar de cifrado avanzado (AES) en el modelo de seguridad basado en el usuario de SNMP.

RFC 5343. Protocolo de administración de red simple (SNMP) Context EngineID Discovery.

BIBLIOGRAFÍA

[1] Zhang J., "*Design and implementation of test IP network intelligent monitoring system based on SNMP*", 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Page s: 2124 - 2127

[2] Palazón Francisco Javier, "*Comparativa sistemas de monitorización cloud*", 18 de mayo de 2018, Revista Byte TI, Recuperado: https://www.revistabyte.es/comparativa-byte-ti/comparativa-sistemas-de-monitorizacion-cloud-2018/

[3] Goralski Walter, "*The Illustrated Network (Second Edition), How TCP/IP Works in a Modern Network, Chapter 28 - Simple Network Management Protocol",* 2017, Pages 707-729, Recuperado de: https://doi.org/10.1016/B978-0-12-811027-0.00028-X

[4] Junco Romero Gerardo y Rabelo Padua Sonia, "*Los recursos de red y su monitoreo, Network resources and its monitoring",* 2018, Revista Cubana de Informática Médica, Universidad Virtual de Salud, Biblioteca virtual de salud, Volumen 18, Número 1, ISSN 1684-1859

[5] Cuchala Sara C., *"Gestión y monitoreo de la red interna del Gobierno Provincial de Imbabura mediante el modelo de gestión ISO y software libre",* 2016, Repositorio Digital Universidad Técnica del Norte, UTN Acreditada, Ibarra, Ecuador, Recuperado de: http://repositorio.utn.edu.ec/handle/123456789/7184

[6] Lee Sihyung, Levanti Kyriaki y Kim Hyong S., *"Networking monitoring: Present and future",* 2014, ScienceDirect, Computer Networks, Volume 65, Pages (84-98), Recuperado de: https://doi.org/10.1016/j.comnet.2014.03.007

[7] Roohi Arman, Raeisifard Khashayar y Ibrahim Suhaimi, *"An application for management and monitoring the data centers based on SNMP",* 2014, IEEE Xplore Digital Library, Batu Ferringhi, Malaysia, Recuperado de: https://ieeexplore.ieee.org/document/7072941

[8] Dordoigne José, "Redes informáticas Nociones Fundamentales (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IPv6...)", 5ª. Edición, Ediciones ENI, 602 p; ISBN 978-2-7460-9733-9.

[9] Ariganello Ernesto, “Redes Cisco – Guía de estudio para la certificación CCNA Routing y Switching”, 4ª. Edición actualizada, Bogotá: Ediciones de la U, 2016 – Madrid, España Ra-ma Editorial, 572 p; ISBN 978-958-762-623-0.

[10] Molero M. Sc. Luis, “Planificación y Gestión de Red”, 1ª. Edición, Universidad “Dr. Rafael Belloso Chacín”, Maracaibo, Venezuela, 2010.

[11] Ariganello Ernesto, “Redes Cisco – Guía de estudio para la certificación CCNA Routing y Switching”, 4ª. Edición actualizada, Bogotá: Ediciones de la U, 2016 – Madrid, España Ra-ma Editorial, 572 p; ISBN 978-958-762-623-0.

[12] Boronat Seguí Fernando – Mario Montagud Climent, Routing y Switching”, “Direccionamiento e interconexión de redes basada en TCP/IP (IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF)” 1era edición, 2013, Editorial Universitat Politécnica de Valéncia, 175 p; ISBN 978-84-9048-037-3.

[13] Kurose James F., Ross Keith W., “Computer Networking”, Seventh Edition, PEARSON 2017, ISBN-13: 978-0-13-359414-0

[14] Abdullah MK – Abdalla MF – Abas AF – Amouzad G., “Multiplexación por división en ciclo de trabajo (DCDM): una novedosa y económica técnica de multiplexación óptica y demultiplexación eléctrica para redes de fibra óptica de alta velocidad”, 2007 Conferencia internacional IFIP sobre redes de comunicaciones inalámbricas y ópticas, Editorial IEEE, DOI: 10.1109 / WOCN.2007.4284149.

[15] Li Tingshun – Zhu Weiying – Xu Jiaohui – Cheng Yongqiang, “El análisis e implementación de la transmisión de datos multiplataforma basada en UDP”, 2012 2ª Conferencia internacional sobre electrónica de consumo, comunicaciones y redes (CECNet), Editorial IEEE, DOI: 10.1109 / CECNet.2012.6201752.

[16] Orphanos G. – Malataras A. – Mountzouris I. – Kanellopoulos D. – Mandalos L. – Koubias S. – Papadopoulos G., “Requisitos informáticos cliente-servidor de los servicios multimedia en red”, Seminario internacional sobre computación cliente / servidor. Actas del seminario (Recopilación No. 1995/184), Editorial IET, DOI: 10.1049 / ic: 19951130.

[17] Serain D., “Cliente / servidor: ¿Por qué? ¿Qué? ¿Cómo?”, Seminario internacional sobre computación cliente / servidor. Actas del seminario (Recopilación No. 1995/184), Editorial IET, DOI: 10.1049 / ic: 19951128.

[18] Nuangjamnong C. – Maj SP – Ternera D., “El modelo de gestión de red OSI-capacidad y gestión del rendimiento”, 2008 IV Conferencia Internacional IEEE sobre Gestión de la Innovación y la Tecnología, Editorial IEEE, DOI: 10.1109 / ICMIT.2008.4654552.

[19] Duan Chenyue – Zhao Qin – Ma Yan, “Modelo de gestión de red distribuida IPV4 / IPV6 orientado a objetos”, 2010 3ª Conferencia internacional IEEE sobre redes de banda ancha y tecnología multimedia (IC-BNMT), Editorial IEEE, DOI: 10.1109 / ICBNMT.2010.5705087.

[20] Case JD, “Gestión de redes de alta velocidad con el protocolo simple de gestión de red (SNMP)”, [1990] Proceedings. 15ª Conferencia sobre Redes de Computadoras Locales, Editorial IEEE, DOI: 10.1109 / LCN.1990.128659.

[21] IEEE Std 802.3.1-2011, “802.3.1-2013 - Estándar IEEE para definiciones de base de información de administración (MIB) para Ethernet”, DOI: 10.1109 / IEEESTD.2013.657279.

[22] Lu Yili – Qian Shao, “Investigación sobre la teoría de SNMP y la tecnología de programación SNMP”, 2010 3ª Conferencia internacional sobre informática y tecnología de la información, Editorial IEEE, DOI: 10.1109 / ICCSIT.2010.5564113.

[23] Jukic O. – Hedi I. – Speh I., “Gestión de fallos y base de información de gestión (MIB)”, 2017 40 Convención internacional sobre tecnología de la información y la comunicación, electrónica y microelectrónica (MIPRO), Editorial IEEE, DOI: 10.23919 / MIPRO.2017.7973468.

[24] SNMP Research International, Inc. Recuperado: http://www.snmp.com/protocol/

[25] Arriola Navarrete Oscar - Tecuatl Quechol Graciela – González Herrera Guadalupe, “Software propietario vs software libre: una evaluación de sistemas integrales para la automatización de bibliotecas”, Investigación Bibliotecológica, Vol.25, Número 54, mayo/agosto 201, México, ISSN: 0187-358X, pp. 37-70

[26] PRTG Network Monitor, Recuperado: https://www.es.paessler.com/

[27] SolarWinds, Recuperado: https://www.solarwinds.com/es/

[28] WhaysUp Gold, “IPSwitch – Software de monitoreo de redes”. Recuperado: https://www.ipswitch.com/monitoreo-de-redes

[29] CACTI, Recuperado: https://www.cacti.net/

[30] Pandora FMS, Recuperado: https://pandorafms.org/es/

[31] THE OPENNMS GROUP, Recuperado: https://www.opennms.org/en

[32] El Sistema operativo GNU, Recuperado: https://www.gnu.org/

[33] Amazon CloudWatch, Recuperado: https://aws.amazon.com/es/cloudwatch/

[34]ZOHO - Gestión de TI, Recuperado: https://www.zoho.com/it-management/?src=top-header&ireft=zohoone

[35] IBM – Gestión de eventos en la nube, Recuperado: https://www.ibm.com/us-en/marketplace/cloud-event-management?lnk=ushpv18t1&lnk2=trial_mkt_CloudEvntMgnt&psrc=none&pexp=def

[36] Interbel, Recuperado: https://www.interbel.es/sobre-nosotros/

[37] Mao Huaqing - Zhu Li - Qin Hang, “Una investigación comparativa sobre SSL VPN y IPSec VPN”, 2012 8ª Conferencia internacional sobre comunicaciones inalámbricas, redes y computación móvil, Editorial IEEE, DOI: 10.1109 / WiCOM.2012.6478270.

[38] Liu Alex X. - Gouda Mohamed G., “Consultas de política de firewall”, Transacciones IEEE en sistemas paralelos y distribuidos (Volumen: 20, Número: 6, junio de 2009), Editorial IEEE, DOI: 10.1109 / TPDS.2008.263.

[39] Papagrigoriou A. - Petrakis P. - Grammatikakis MD, “Un módulo firewall resolviendo consistencia de reglas”, 2017 13 ° Taller sobre soluciones inteligentes en sistemas integrados (WISES), Editorial IEEE, DOI: 10.1109 / WISES.2017.7986931.

[40] Tihomir Katic - Predrag Pale, “Optimization of Firewall Rules”, 2007 29th International Conference on Information Technology Interfaces, Editorial IEEE, DOI: 10.1109/ITI.2007.4283854.

[41] Axarnet, Recuperado: https://www.axarnet.es/

[42] Yagues Fernández Pablo, “Programación de redes SDN mediante el controlador POX”, Universidad Politécnica de Cartagena, Escuela Técnica Superior de Ingeniería de Telecomunicación, Proyecto fin de carrera, Octubre 2015.

[43] Wei Tsai Pang – Wei Tsai Chun – Wei Hsu Chia – Sing Yang Chu, “Monitoreo de redes en redes definidas por software: una revisión”, IEEE Systems Journal, Volume 12, Issue 4, Diciembre 2018, Editorial IEEE, DOI: 10.1109 / JSYST.2018.2798060.

[44] Dalibalta Dina, “SNMP MIB para OpenFlow-Capable Switch”, Universidad de Houston, Facultad de Ingeniería de Tecnología, Proyecto para el grado de magister, Diciembre 2015.

[45] Benzekki Karnal – El Fergougui Abdeslam – Abdelbaki – Elalaoui Elbelrhiti, “Redes de finidas por software (SDN): una encuesta”, Laboratorio de Redes y Sistemas Informáticos, Departamento de Matemáticas y Ciencias de la Computación, Facultad de Ciencias, Universidad Moulay Ismail – Meknes - Marruecos, Redes de Seguridad y Comunicación, Biblioteca en línea de Wiley, 7 de febrero 2017, DOI: 10.1002 / sec.1737.

[46] Kreutz Diego – Ramos Fernando M. V. – Esteves Veríssimo Paulo – Esteve Rothenberg Christian - Azodolmolky Siamak - Uhlig Steve, “Redes definidas por software (SDN): una encuesta exhaustiva”, Actas del IEEE (Volumen: 103, Número: 1, enero de 2015), 19 de diciembre de 2014, DOI: 10.1109 / JPROC.2014.2371999.

[47] Fonseca Paulo César da Rocha – Souza Mota Edjard, “Una encuesta sobre la gestión de fallos en redes definidas por software”, IEEE Communications Surveys & Tutorials (Volumen: 19, Número: 4, Cuarto trimestre de 2017), 26 de junio de 2017, DOI: 10.1109 / COMST.2017.2719862.